Qualys. Enterprise TruRisk™ Platform

Scan Results

July 01, 2025

Report Summary	
User Name:	Oscar Bevoni
Login Name:	grupp5sb
Company:	Cyberinova Ltd
User Role:	Manager
Address:	
City:	
Zip:	
Country:	
Created:	01/07/2025 at 10:53:17 PM (GMT+0200)
Launch Date:	01/07/2025 at 10:08:34 PM (GMT+0200)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1751400514.86815
External Scanners:	64.39.106.108 (Scanner 14.8.11-1, Vulnerability Signatures 2.6.362-2)
Duration:	00:35:40
Title:	I-Mesh Jitsi-Gtw AWS - (normal exposure) - 20250701
Network:	Global Default Network
Asset Groups:	-
IPs:	
Excluded IPs:	-
FQDNs:	jitsi-gtw.inovamesh.cloud
Options Profile:	I-Mesh Option Profile (Oscar)

Summary of Vulnerabilities

Vulnerabilities Total	40

Security Risk (Avg)	3.0

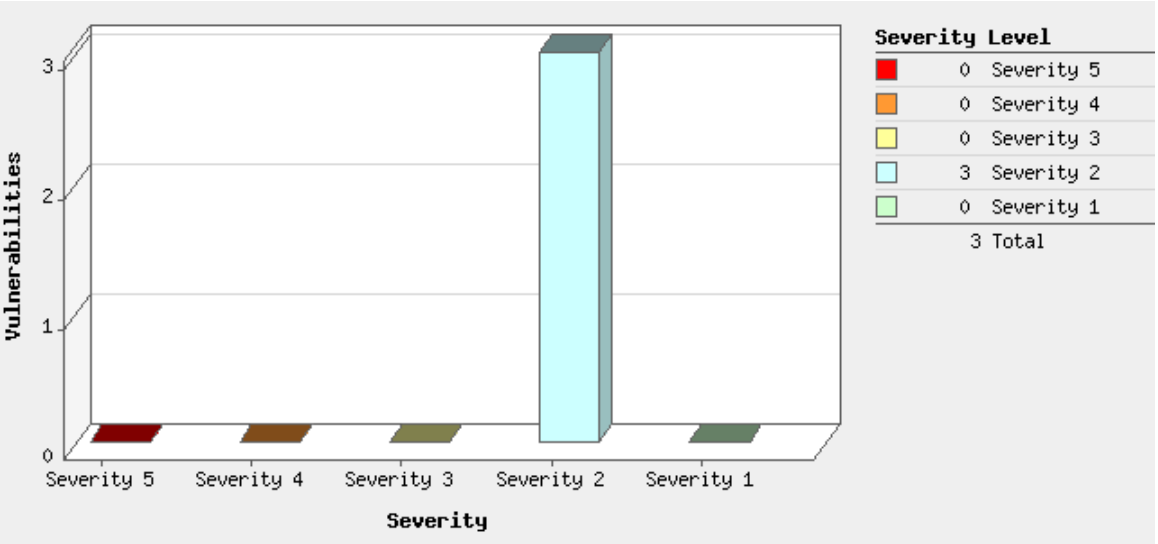
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	2	2	4
2	3	2	4	9
1	0	0	27	27
Total	3	4	33	40

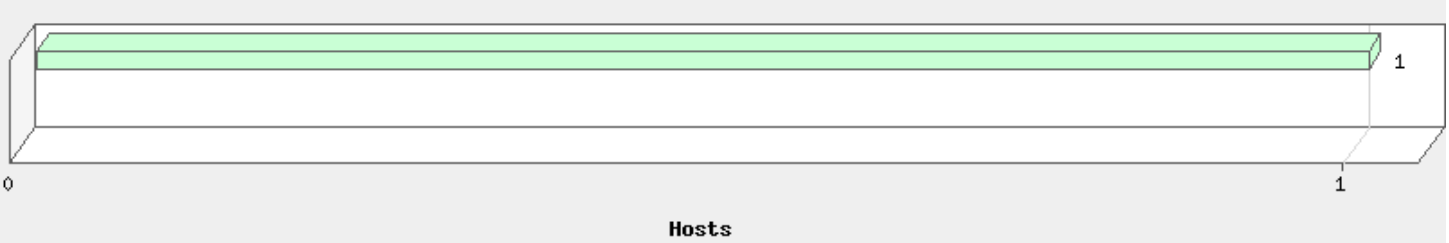
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	15	15
General remote services	3	0	7	10
CGI	0	4	2	6
Web server	0	0	4	4
TCP/IP	0	0	4	4
Total	3	4	32	39

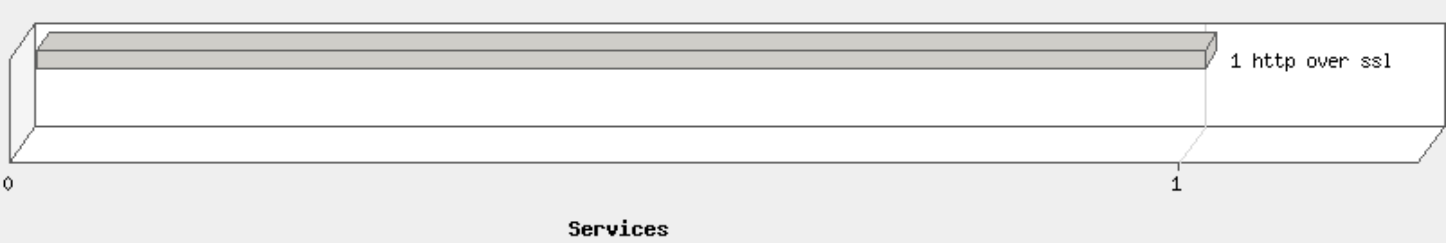
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

52.18.123.250 (jitsi-gtw.inovamesh.cloud, -)
Global Default Network

Vulnerabilities (3)

2 SSL Certificate - Self-Signed Certificate — port 443/tcp over SSL

QID:	38169	CVSS Base:	6.4 [1]
Category:	General remote services	CVSS Temporal:	4.7
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	23/11/2020	CVSS3.1 Base:	6.5 [1]
User Modified:	-	CVSS3.1 Temporal:	5.3

Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 emailAddress=webmaster@jitsi-gtw.inovamesh.cloud,CN=jitsi-gtw.inovamesh.cloud,OU=jitsi-gtw,O=inovamesh.cloud is a self signed certificate.

2 SSL Certificate - Signature Verification Failed Vulnerability

port 443/tcp over SSL

QID:	38173	CVSS Base:	6.4 [1]
Category:	General remote services	CVSS Temporal:	4.7
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	28/02/2022	CVSS3.1 Base:	6.5 [1]
User Modified:	-	CVSS3.1 Temporal:	5.6
Edited:	No		
PCI Vuln:	Yes		

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 emailAddress=webmaster@jitsi-gtw.inovamesh.cloud,CN=jitsi-gtw.inovamesh.cloud,OU=jitsi-gtw,O=inovamesh.cloud
ISSUER:_emailAddress=webmaster@jitsi-gtw.inovamesh.cloud,CN=jitsi-gtw.inovamesh.cloud,OU=jitsi-gtw,O=inovamesh.cloud self signed certificate

2 SSL Certificate - Invalid Maximum Validity Date Detected port 443/tcp over SSL

QID:	38685	CVSS Base:	6.4 [1]
Category:	General remote services	CVSS Temporal:	5.2
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	14/04/2021	CVSS3.1 Base:	6.5 [1]
User Modified:	-	CVSS3.1 Temporal:	5.8
Edited:	No		
PCI Vuln:	Yes		

THREAT:

Subscriber Certificates issued on or after 1 September 2020 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days. (13 months)
Subscriber Certificates issued after 1 March 2018, but prior to 1 September 2020, MUST NOT have a Validity Period greater than 825 days. (27 months)
Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST NOT have a Validity Period greater than 39 months.
SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently.

It is detected that maximum validity of certificate on the system is more than what is recommended.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with recommended maximum validity.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 emailAddress=webmaster@jitsi-gtw.inovamesh.cloud,CN=jitsi-gtw.inovamesh.cloud,OU=jitsi-gtw,O=inovamesh.cloud
ISSUER:_emailAddress=webmaster@jitsi-gtw.inovamesh.cloud,CN=jitsi-gtw.inovamesh.cloud,OU=jitsi-gtw,O=inovamesh.cloud is valid for more than 398 days

Potential Vulnerabilities (4)

3 Nginx Specially Crafted MP4 Vulnerability (CVE-2024-7347) port 443/tcp

QID:	732378	CVSS Base:	0.0 [1]
Category:	CGI	CVSS Temporal:	0.0
Associated CVEs:	CVE-2024-7347		
Vendor Reference:	NGINX Security Advisory		
Bugtraq ID:	-		
Service Modified:	16/05/2025	CVSS3.1 Base:	4.7
User Modified:	-	CVSS3.1 Temporal:	4.1
Edited:	No		
PCI Vuln:	No		

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A security issue was identified in the ngx_http_mp4_module, which might allow an attacker to cause a worker process crash by using a specially crafted mp4 file.

Affected Versions:
Nginx version from 1.5.13 prior to 1.26.2
Nginx version from 1.27.0 prior to 1.27.1

IMPACT:

Successful exploitation of the vulnerability allows an attacker to cause a worker process crash by using a specially crafted mp4 file .

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 443 .
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Jul 2025 20:15:45 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Strict-Transport-Security: max-age=63072000

<GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

3 Nginx Specially Crafted MP4 Vulnerability (CVE-2024-7347) port 443/tcp over SSL

QID:	732378	CVSS Base:	0.0 [1]
Category:	CGI	CVSS Temporal:	0.0
Associated CVEs:	CVE-2024-7347		
Vendor Reference:	NGINX Security Advisory		
Bugtraq ID:	-		
Service Modified:	16/05/2025	CVSS3.1 Base:	4.7
User Modified:	-	CVSS3.1 Temporal:	4.1
Edited:	No		
PCI Vuln:	No		

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A security issue was identified in the ngx_http_mp4_module, which might allow an attacker to cause a worker process crash by using a specially crafted mp4 file.

Affected Versions:
Nginx version from 1.5.13 prior to 1.26.2
Nginx version from 1.27.0 prior to 1.27.1

IMPACT:

Successful exploitation of the vulnerability allows an attacker to cause a worker process crash by using a specially crafted mp4 file .

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Jul 2025 20:13:49 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
Strict-Transport-Security: max-age=63072000

```
<html itemscope itemtype="http://schema.org/Product" prefix="og: http://ogp.me/ns#" xmlns="http://www.w3.org/1999/html">
  <head>

    <meta charset="utf-8">
    <meta http-equiv="content-type" content="text/html;charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0">
    <meta name="theme-color" content="#2A3A4B">
    <base href="/" />


    <link rel="apple-touch-icon" href="images/apple-touch-icon.png">
    <link rel="stylesheet" href="css/all.css?v=8542">
```

```
<link rel="manifest" id="manifest-placeholder">

<script>
   function contextRoot(pathname) {
      const contextRootEndIndex = pathname.lastIndexOf('/');

      return (
         contextRootEndIndex === -1
         ? '/'
         : pathname.substring
```

2 Nginx Certificate Authentication Bypass Vulnerability (CVE-2025-23419) port 443/tcp

QID:	732377	CVSS Base:	0.0 [1]
Category:	CGI	CVSS Temporal:	0.0
Associated CVEs:	CVE-2025-23419		
Vendor Reference:	NGINX Security Advisory		
Bugtraq ID:	-		
Service Modified:	16/05/2025	CVSS3.1 Base:	4.3
User Modified:	-	CVSS3.1 Temporal:	3.8
Edited:	No		
PCI Vuln:	Yes		

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A problem with SSL session resumption in nginx was identified.

Affected Versions:
Nginx version from 1.11.4 prior to 1.26.3
Nginx version from 1.27.0 prior to 1.27.4

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 443 .
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Jul 2025 20:15:45 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

Vary: Accept-Encoding
Strict-Transport-Security: max-age=63072000

<GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

2 Nginx Certificate Authentication Bypass Vulnerability (CVE-2025-23419) port 443/tcp over SSL

QID:	732377	CVSS Base:	0.0 [1]
Category:	CGI	CVSS Temporal:	0.0
Associated CVEs:	CVE-2025-23419		
Vendor Reference:	NGINX Security Advisory		
Bugtraq ID:	-		
Service Modified:	16/05/2025	CVSS3.1 Base:	4.3
User Modified:	-	CVSS3.1 Temporal:	3.8
Edited:	No		
PCI Vuln:	Yes		

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A problem with SSL session resumption in nginx was identified.

Affected Versions:
Nginx version from 1.11.4 prior to 1.26.3
Nginx version from 1.27.0 prior to 1.27.4

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Jul 2025 20:13:49 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
Strict-Transport-Security: max-age=63072000

<html itemscope itemtype="http://schema.org/Product" prefix="og: http://ogp.me/ns#" xmlns="http://www.w3.org/1999/html">
<head>

```
<meta charset="utf-8">
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0">
<meta name="theme-color" content="#2A3A4B">
<base href="/" />


<link rel="apple-touch-icon" href="images/apple-touch-icon.png">
<link rel="stylesheet" href="css/all.css?v=8542">

<link rel="manifest" id="manifest-placeholder">

<script>
   function contextRoot(pathname) {
      const contextRootEndIndex = pathname.lastIndexOf('/');

      return (
         contextRootEndIndex === -1
         ? '/'
         : pathname.substring
```

Information Gathered (33)

3 DEFLATE Data Compression Algorithm Used for HTTPS

QID:	42416
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/08/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

3 Content-Security-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48001
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	11/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	29/05/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 39 days, 3 hours, and 0 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Web Applications and Plugins Detected port 443/tcp

QID:	45114
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/01/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The result section of this QID lists web applications and plugins that were detected on the target using web application fingerprinting. This technique compares static files at known locations against precomputed hashes for versions of those files in all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.

Following open source and free applications are currently supported:
Joomla!
MediaWiki
WordPress
phpBB
MovableType
Drupal
osCommerce
PHP-Nuke
Moodle
Liferay
Tikiwiki
Twiki
phpmyadmin
SPIP
Confluence(free versions)
Wikka
Wacko
Usemod
e107
Flyspray
AppRain
V-CMS
AjaxPlorer/Pydio
eFront Learning Management System
vTigerCRM (Open source versions)
MyBB
WebCalendar

PivotX WebLog
DokuWiki
MODX Revolution
MODX Evolution
Collabtive
Achievo
Magento 1.x CE
iCE Hrm (Opensource Version)
AdaptCMS
ownCloud
HumHub
Redaxscript
phpwcms
Wolf CMS
Pligg CMS
Zen Cart
Xoops
TYPO3
Microweber

This QID is based on the Blind Elephant project (http://blindelephant.sourceforge.net/). For a complete list of supported web applications and plugins, please check the following link: DOC-5480 (https://community.qualys.com/docs/DOC-5480).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

moin	1.9.8	in directory: /	Source: /moin_static173/robots.txt

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 443/tcp over SSL

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server Supports HTTP 2 on 443 port.

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/01/2018
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
52.18.123.250	jitsi-gtw.inovamesh.cloud
52.18.123.250	ec2-52-18-123-250.eu-west-1.compute.amazonaws.com

1 Firewall Detected

QID:	34011
Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	22/04/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-27,29,31,33,35,37-39,41-223,225,242-246,256-265,
280-282,309,311,318,322-325,340,344-351,363,369-381,383-442,444-581,587,
592-593,598,600,606-620,623-624,626-627,631,633-637,646,666-675,685,700,
704-705,707,709-711,729-731,740-742,744,747-754,758-765,767,769-777,780-783,
786,789,799-801,805-806,808,830,843,860,873,880,886-888,900-902,911,943,
950,954-955,990-1001,1008,1010-1012,1015,1022-1100,1109-1112,1114,1119,
1123,1155,1167,1170,1177,1194,1200,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1250,1269,1290,1311,1313-1314,1337,1344-1625,1636-1774,
1776-1815,1818-1824,1830,1833,1883,1900-1909,1911-1920,1935,1944, and more.
We have omitted from this list 1645 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	15/08/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: NET-52-16-0-0-1
Network description:
Amazon Data Services Ireland Limited AMAZON-DUB

1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	27/09/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: NET-140-91-0-0-2
ISP Network description:
Oracle Public Cloud OC-195

 1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/05/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	140.91.222.68	0.14ms	ICMP	
2	72.21.221.57	0.83ms	ICMP	
3	*.*.*.*	0.00ms	Other	443
4	*.*.*.*	0.00ms	Other	443
5	*.*.*.*	0.00ms	Other	443
6	*.*.*.*	0.00ms	Other	443
7	*.*.*.*	0.00ms	Other	443
8	52.18.123.250	18.78ms	TCP	443

 1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	15/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2132 seconds

Start time: Tue, Jul 01 2025, 20:09:09 GMT

End time: Tue, Jul 01 2025, 20:44:41 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	27/08/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
jitsi-gtw.inovamesh.cloud	User-provided DNS
ec2-52-18-123-250.eu-west-1.compute.amazonaws.com	FQDN

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	24/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	443	3:48:51

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	19/12/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
443	https	http protocol over TLS/SSL	http over ssl	

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	19/11/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1089037100 with a standard deviation of 506240806. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5098 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	27/07/2006
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 443: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 25 milli seconds

1 Nginx Web Server Detected port 443/tcp

QID:	45433
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	15/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 443 over TCP.
Server: nginx/1.24.0 (Ubuntu)

1 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/07/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	20/07/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

```
GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive


HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Jul 2025 20:15:45 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Strict-Transport-Security: max-age=63072000
```

 1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	18/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.
GET / HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/06/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=63072000

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/09/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/phprojekt-3.1/lang/	brute force
/images/	brute force
/phprojekt-3.1a/lang/	brute force
/phprojekt/lang/	brute force
/css/	brute force
/phpMyAdmin-2.5.1/css/	brute force
/css/	web page
/images/	web page
/libs/	web page
/static/	brute force

1 Apache Default Foreign Language File Still on Server port 443/tcp

QID:	86743
Category:	Web server

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/07/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: jitsi-gtw.inovamesh.cloud
Connection: Keep-Alive

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	16/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /
HTTP/1.1Host:
jitsi-gtw.inovamesh.cloudConnection:
Keep-Alive

HTTP/1.1 200
OKServer: nginx/1.24.0
(Ubuntu)Date: Tue, 01 Jul 2025 20:15:45
GMTContent-Type:
text/htmlTransfer-Encoding:
chunkedConnection:
keep-aliveVary:
Accept-EncodingStrict-Transport-Security:
max-age=63072000
<html itemscope itemtype="http://schema.org/Product" prefix="og: http://ogp.me/ns#"
xmlns="http://www.w3.org/1999/html">
<head>
<meta
charset="utf-8"> <meta http-equiv="content-type"
content="text/html;charset=utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0,
maximum-scale=1.0"> <meta name="theme-color"
content="#2A3A4B"> <base href="/"
/>

<link rel="apple-touch-icon"
href="images/apple-touch-icon.png"> <link rel="stylesheet"
href="css/all.css?v=8542">
<link rel="manifest"
id="manifest-placeholder">

<script> function contextRoot(pathname)
{ const contextRootEndIndex =
pathname.lastIndexOf('/');
return
(contextRootEndIndex ===
-1 ?
'/' : pathname.substring(0, contextRootEndIndex +
1)
);
} window.EXCALIDRAW_ASSET_PATH =
'libs/'; // Dynamically generate the manifest location URL. It must be served from the document origin, and we may
have // the base pointing to the CDN. This way we can generate a full URL which will bypass the
base. document.querySelector('#manifest-placeholder').setAttribute('href', window.location.origin + contextRoot(window.location.pathname) +
'manifest.json');
document.addEventListener('DOMContentLoaded', () =>
{ if (!JitsiMeetJS.app)
{
return;
}

JitsiMeetJS.app.renderEntryPoint({ Component:
JitsiMeetJS.app.entryPoints.APP
})
const isEmbedded = () =>
{ try
{ return window.self !==
window.top; } catch (e)
{ return
true;
}

```
};
const isElectron =
navigator.userAgent.includes('Electron');            const shouldRegisterWorker = !isElectron && !isEmbedded() && 'serviceWorker' in
navigator;
if (shouldRegisterWorker)
{
navigator.serviceWorker                    .register(window.location.origin + contextRoot(window.location.pathname) +
'pwa-worker.js')                  .then(reg =>
{                      console.log('Service worker registered.',
reg);
})                  .catch(err =>
{
console.log(err);
});
}
});
</script>
<script>        // IE11 and earlier can be identified via their user agent and
be        // redirected to a page that is known to have no newer js
syntax.        if (window.navigator.userAgent.match(/(MSIE|Trident)/))
{           var roomName =
encodeURIComponent(window.location.pathname);            window.location.pathname =
'static/recommendedBrowsers.html';
}
window.indexLoadedTime =
window.performance.now();        console.log("(TIME) index.html loaded:\t",
indexLoadedTime);        window.addEventListener('load', function()
{           window.loadedEventTime =
window.performance.now();            console.log("(TIME) window loaded event:\t",
loadedEventTime);
});
// XXX the code below listeners for errors and displays an error
message        // in the document body when any of the required files fails to
load.        // The intention is to prevent from displaying broken
page.        var criticalFiles =
[
"config.js",
"utils.js",
"do_external_connect.js",
"interface_config.js",
"lib-jitsi-meet.min.js",
"app.bundle.min.js",
"all.css?v=8542"
];        var loadErrHandler = function(e)
{           var target =
e.target;            // Error on <script> and
<link>(CSS)            // <script> will have .src and <link>
.href            var fileRef = (target.src ? target.src :
target.href);            if (("SCRIPT" === target.tagName || "LINK" ===
target.tagName)                &&
criticalFiles.some(                    function(file) { return fileRef.indexOf(file) !== -1 }))
{               window.onload = function()
{                   // The whole complex part below implements page reloads
with                    // "exponential backoff". The retry attempt is passes
as                  // "rCounter" query
parameter                    var href =
window.location.href;
var retryMatch =
href.match(/.+(\?|&)rCounter=(\d+)/);                    var retryCountStr = retryMatch ? retryMatch[2] :
"0";                    var retryCount =
Number.parseInt(retryCountStr);
if (retryMatch == null)
{                       var separator = href.indexOf("?") === -1 ? "?" :
"&";                        var hashIdx =
href.indexOf("#");
if (hashIdx === -1)
{                           href += separator +
"rCounter=1";                        } else
{                           var hashPart =
href.substr(hashIdx);
href = href.substr(0,
hashIdx)                              + separator + "rCounter=1" +
hashPart;
}                   } else
{                       var separator =
retryMatch[1];
href =
href.replace(
```

```
/(\?|&)rCounter=(\d+)/,                         separator + "rCounter=" + (retryCount +
1));
}
var delay = Math.pow(2, retryCount) *
2000;                   if (isNaN(delay) || delay < 2000 || delay >
60000)                      delay =
10000;
var showMoreText = "show
more";                   var showLessText = "show
less";

document.body.innerHTML                         = "<div
style='"                      + "position: absolute;top: 50%;left:
50%;"                     + "text-align:
center;"                      + "font-size:
medium;"                        + "font-weight:
400;"                     + "transform: translate(-50%,
-50%)'>"                       + "Uh oh! We couldn't fully download everything we needed
:("                    + "<br/>
"                   + "We will try again shortly. In the mean time, check for problems with your Internet
connection!"                        + "<br/><br/>
"                   + "<div id='moreInfo'
style='"                      + "display: none;'>" + "Missing " +
fileRef                     +
"<br/><br/></div>"                        + "<a id='showMore'
style='"                      + "text-decoration:
underline;"                         +
"font-size:small;"                          + "cursor: pointer'>" + showMoreText +
"</a>"                      +
""                     + "<a id ='reloadLink'
style='"                      + "text-decoration:
underline;"                         +
"font-size:small;"                          + "'>reload
now</a>"                        +
"</div>";
var reloadLink =
document.getElementById('reloadLink');                    reloadLink.setAttribute('href',
href);
var showMoreElem =
document.getElementById("showMore");                    showMoreElem.addEventListener('click', function ()
{                       var
moreInfoElem                                    =
document.getElementById("moreInfo");
if (showMoreElem.innerHTML === showMoreText)
{
moreInfoElem.setAttribute(
"style",                                  "display:
block;"                                   +
"color:#FF991F;"                                    +
"font-size:small;"                                  +
"user-select:text;");                               showMoreElem.innerHTML =
showLessText;
}                       else
{
moreInfoElem.setAttribute(                                      "style", "display:
none;");                              showMoreElem.innerHTML =
showMoreText;
}
});

window.setTimeout(                      function () { window.location.replace(href); },
delay);
// Call extra handler if
defined.                    if (typeof postLoadErrorHandler === "function")
{
postLoadErrorHandler(fileRef);
}
};
window.removeEventListener(                     'error', loadErrHandler, true /* capture phase
*/);
}
};
window.addEventListener(            'error', loadErrHandler, true /* capture phase type of listener
*/);
</script>    <script>/* eslint-disable comma-dangle, no-unused-vars, no-var, prefer-template, vars-on-top
*/
/*
* NOTE: If you add a new option please remember to document it
```

```
here: *
https://jitsi.github.io/handbook/docs/dev-guide/dev-guide-configuration
*/
var subdir =
'';var subdomain =
'';
if (subdomain)
{    subdomain = subdomain.substr(0, subdomain.length -
1).split('.')
.join('_')        .toLowerCase() +
'.';}

// In case of no ssi provided by the webserver, use empty
stringsif (subdir.startsWith('<!--'))
{    subdir =
'';}
if (subdomain.startsWith('<!--'))
{    subdomain =
'';}

var enableJaaS =
false;
var config =
{    //
Connection
//
hosts:
{        // XMPP
domain.        domain:
'jitsi-gtw.inovamesh.cloud',
// When using authentication, domain for guest
users.        // anonymousdomain:
'guest.example.com',
// Domain for authenticated users. Defaults to
<domain>.        // authdomain:
'jitsi-gtw.inovamesh.cloud',
// Focus component domain. Defaults to
focus.<domain>.        // focus:
'focus.jitsi-gtw.inovamesh.cloud',
// XMPP MUC domain. FIXME: use XEP-0030 to discover
it.        muc: 'conference.' + subdomain +
'jitsi-gtw.inovamesh.cloud',
},
// BOSH URL. FIXME: use XEP-0156 to discover
it.    bosh: 'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'http-bind',
// Websocket URL
(XMPP)    websocket: 'wss://jitsi-gtw.inovamesh.cloud/' + subdir +
'xmpp-websocket',
// websocketKeepAliveUrl: 'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'_unlock',
// Whether BOSH should be preferred over WebSocket if both are
configured.    // preferBosh:
false,
// The real JID of focus participant - can be overridden
here    // Do not change username - FIXME: Make focus username
configurable    //
https://github.com/jitsi/jitsi-meet/issues/7376    // focusUserJid:
'focus@auth.jitsi-gtw.inovamesh.cloud',
// Option to send conference requests to jicofo over http (requires nginx rule for
it)    //
conferenceRequestUrl:    //   'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'conference-request/v1',
// Options related to the bridge (colibri) data
channel    bridgeChannel:
{        // If the backend advertises multiple colibri websockets, this options
allows        // to filter some of them out based on the domain name. We use the first
URL        // which does not match ignoreDomain, falling back to the first one that
matches        // ignoreDomain. Has no effect if
undefined.        // ignoreDomain:
'example.com',
// Prefer SCTP (WebRTC data channels over the media path) over a colibri
websocket.        // If SCTP is available in the backend it will be used instead of a WS. Defaults
to        // false (SCTP is used only if available and no WS are
available).        // preferSctp:
false
},
// Testing / experimental
```

```
features.
//
testing:
{       // Allows the setting of a custom bandwidth value from the
UI.       // assumeBandwidth:
true,
// Enables use of getDisplayMedia in
electron       // electronUseGetDisplayMedia:
false,
// Enables the use of the codec selection API supported by the browsers
.       // enableCodecSelectionAPI:
false,
// P2P test mode disables automatic switching to P2P when there are
2       // participants in the
conference.       // p2pTestMode:
false,
// Enables the test specific features consumed by
jitsi-meet-torture       // testMode:
false,
// Disables the auto-play behavior of *all* newly created video
element.       // This is useful when the client runs on a host with limited
resources.       // noAutoPlayVideo:
false,
// Experiment: Whether to skip interim
transcriptions.       // skipInterimTranscriptions:
false,
// Dump transcripts to a <transcript> element for
debugging.       // dumpTranscript:
false,
// Log the audio
levels.       // debugAudioLevels:
true,
// Will replace ice candidates IPs with invalid ones in order to fail
ice.       // failICE:
true,
},
// Disables moderator
indicators.    // disableModeratorIndicator:
false,
// Disables the reactions
feature.    // disableReactions:
true,
// Disables the reactions moderation
feature.    // disableReactionsModeration:
false,
// Disables polls
feature.    // disablePolls:
false,
// Disables demote button from
self-view    // disableSelfDemote:
false,
// Disables self-view tile. (hides it from tile view and from
filmstrip)    // disableSelfView:
false,
// Disables self-view settings in
UI    // disableSelfViewSettings:
false,
// screenshotCapture :
{    //      Enables the screensharing capture
feature.    //      enabled:
false,
//    //      The mode for the screenshot capture
feature.    //      Can be either 'recording' - screensharing screenshots are
taken    //      only when the recording is also
on,    //      or 'always' - screensharing screenshots are always
taken.    //      mode:
'recording',    //
}
// Disables ICE/UDP by filtering out local and remote UDP candidates
in    //
signalling.    // webrtcIceUdpDisable:
false,
// Disables ICE/TCP by filtering out local and remote TCP candidates
in    //
signalling.    // webrtcIceTcpDisable:
false,

//
```

```
Media
//
//
Audio
// Disable measuring of audio
levels.    // disableAudioLevels:
false,
// audioLevelsInterval:
200,
// Enabling this will run the lib-jitsi-meet no audio detection module
which    // will notify the user if the current selected microphone has no
audio    // input and will suggest another valid device if one is
present.    enableNoAudioDetection:
true,
// Enabling this will show a "Save Logs" link in the GSM popover that can
be    // used to collect debug information (XMPP IQs, SDP offer/answer
cycles)    // about the
call.    // enableSaveLogs:
false,
// Enabling this will hide the "Show More" link in the GSM popover that can
be    // used to display more statistics about the connection (IP, Port, protocol,
etc).    // disableShowMoreStats:
true,
// Enabling this will run the lib-jitsi-meet noise detection module which
will    // notify the user if there is noise, other than voice, coming from the
current    // selected microphone. The purpose it to let the user know that the input
could    // be potentially unpleasant for other meeting
participants.    enableNoisyMicDetection:
true,
// Start the conference in audio only mode (no video is being received
nor    //
sent).    // startAudioOnly:
false,
// Every participant after the Nth will start audio
muted.    // startAudioMuted:
10,
// Start calls with audio muted. Unlike the option above, this one is
only    // applied locally. FIXME: having these 2 options is
confusing.    // startWithAudioMuted:
false,
// Enabling it (with #params) will disable local audio output of
remote    // participants and to enable it back a reload is
needed.    // startSilent:
false,
// Enables support for opus-red (redundancy for
Opus).    // enableOpusRed:
false,
// Specify audio quality stereo and opusMaxAverageBitrate values in order to enable HD
audio.    // Beware, by doing so, you are disabling echo cancellation, noise suppression and
AGC.    // Specify enableOpusDtx to enable support for opus-dtx
where    // audio packets wont be transmitted while participant is silent or
muted.    // audioQuality:
{    //     stereo:
false,    //     opusMaxAverageBitrate: null, // Value to fit the 6000 to 510000
range.    //     enableOpusDtx:
false,    //
},
// Noise suppression configuration. By default rnnoise is used. Optionally
Krisp    // can be used by enabling it below, but the Krisp JS SDK files must be supplied in
your    // installation. Specifically, these files are
needed:    //   -
https://meet.example.com/libs/krisp/krisp.mjs    //   -
https://meet.example.com/libs/krisp/models/model_8.kw    //   -
https://meet.example.com/libs/krisp/models/model_nc.kw    //   -
https://meet.example.com/libs/krisp/models/model_bvc.kw    //   -
https://meet.example.com/libs/krisp/assets/bvc-allowed.txt    //     In case when you have known BVC supported devices and you want to extend
allowed devices
list    //   -
https://meet.example.com/libs/krisp/assets/bvc-allowed-ext.txt    //     In case when you have known BVC supported devices and you want to extend
allowed devices
list    //   -
https://meet.example.com/libs/krisp/models/model_inbound_8.kw    //   -
https://meet.example.com/libs/krisp/models/model_inbound_16.kw    //     In case when you want to use inbound noise suppression
models    // NOTE: Krisp JS SDK v2.0.0 was
tested.    // noiseSuppression:
{    //     krisp:
{    //         enabled:
false,    //         logProcessStats:
```

```
false,    //        debugLogs:
false,    //        useBVC:
false,    //        bufferOverflowMS:
1000,    //        inboundModels:
{    //            modelInbound8:
'model_inbound_8.kef',    //            modelInbound16:
'model_inbound_16.kef',    //
},    //        preloadInboundModels:
{    //            modelInbound8:
'model_inbound_8.kef',    //            modelInbound16:
'model_inbound_16.kef',    //
},    //        preloadModels:
{    //            modelBVC:
'model_bvc.kef',    //            model8:
'model_8.kef',    //            modelNC:
'model_nc_mq.kef',    //
},    //        models:
{    //            modelBVC:
'model_bvc.kef',    //            model8:
'model_8.kef',    //            modelNV:
'model_nc_mq.kef',    //
},    //        bvc:
{    //            allowedDevices:
'bvc-allowed.txt',    //            allowedDevicesExt:
'bvc-allowed-ext.txt',    //
}    //
},    //
},
//
Video
// Sets the default camera facing
mode.    // cameraFacingMode:
'user',
// Sets the preferred resolution (height) for local video. Defaults to
720.    // resolution:
720,
// DEPRECATED. Please use raisedHands.disableRemoveRaisedHandOnFocus
instead.    // Specifies whether the raised hand will hide when someone becomes a dominant speaker or
not    // disableRemoveRaisedHandOnFocus:
false,
// Specifies which raised hand related config should be
set.    // raisedHands:
{    //    // Specifies whether the raised hand can be lowered by
moderator.    //    disableLowerHandByModerator:
false,
//    // Specifies whether there is a notification before hiding the raised
hand    //    // when someone becomes the dominant
speaker.    //    disableLowerHandNotification:
true,
//    // Specifies whether there is a notification when you are the next speaker in
line.    //    disableNextSpeakerNotification:
false,
//    // Specifies whether the raised hand will hide when someone becomes a dominant speaker or
not.    //    disableRemoveRaisedHandOnFocus:
false,    //
},
// speakerStats:
{    //    // Specifies whether the speaker stats is enable or
not.    //    disabled:
false,
//    // Specifies whether there will be a search field in speaker stats or
not.    //    disableSearch:
false,
//    // Specifies whether participants in speaker stats should be ordered or not, and with what
priority.    //    // 'role', <- Moderators on
top.    //    // 'name', <- Alphabetically by
name.    //    // 'hasLeft', <- The ones that have left in the
bottom.    //    order:
[    //
'role',    //
'name',    //
'hasLeft',    //
],    //
},
// DEPRECATED. Please use speakerStats.disableSearch
instead.    // Specifies whether there will be a search field in speaker stats or
not    // disableSpeakerStatsSearch:
false,
```

```
// DEPRECATED. Please use speakerStats.order
.    // Specifies whether participants in speaker stats should be ordered or not, and with what
priority    // speakerStatsOrder:
[    //  'role', <- Moderators on
top    //  'name', <- Alphabetically by
name    //  'hasLeft', <- The ones that have left in the
bottom    // ], <- the order of the array elements determines
priority
// How many participants while in the tile view mode, before the receiving video quality is reduced from HD to
SD.    // Use -1 to
disable.    // maxFullResolutionParticipants:
2,
// w3c spec-compliant video constraints to use for video capture.
Currently    // used by browsers that return true from
lib-jitsi-meet's    // util#browser#usesNewGumFlow. The constraints are independent
from    // this config's resolution value. Defaults to requesting an
ideal    // resolution of
720p.    // constraints:
{    //     video:
{    //         height:
{    //             ideal:
720,    //             max:
720,    //             min:
240,    //
},    //
},    //
},
// Enable / disable simulcast
support.    // disableSimulcast:
false,
// Every participant after the Nth will start video
muted.    // startVideoMuted:
10,
// Start calls with video muted. Unlike the option above, this one is
only    // applied locally. FIXME: having these 2 options is
confusing.    // startWithVideoMuted:
false,
// Desktop
sharing
// Optional desktop sharing frame rate options. Default value: min:5,
max:5.    // desktopSharingFrameRate:
{    //     min:
5,    //     max:
5,    //
},
// Optional screenshare settings that give more control over screen capture in the
browser.    // screenShareSettings:
{    //      // Show users the current tab is the preferred capture source, default:
false.    //      desktopPreferCurrentTab:
false,    //      // Allow users to select system audio, default:
include.    //      desktopSystemAudio:
'include',    //      // Allow users to seamlessly switch which tab they are sharing without having to select the tab
again.    //      desktopSurfaceSwitching:
'include',    //      // Allow a user to be shown a preference for what screen is to be captured, default:
unset.    //      desktopDisplaySurface:
undefined,    //      // Allow users to select the current tab as a capture source, default:
exclude.    //      desktopSelfBrowserSurface:
'exclude'    //
},
//
Recording
// Enable the dropbox
integration.    // dropbox:
{    //     appKey: '<APP_KEY>', // Specify your app key
here.    //     // A URL to redirect the user to, after
authenticating    //     // by default
uses:    //     //
'https://jitsi-gtw.inovamesh.cloud/static/oauth.html'    //
redirectURI:    //
'https://jitsi-gtw.inovamesh.cloud/subfolder/static/oauth.html',    //
},
// configuration for all things recording related. Existing settings will be migrated here in the
future.    // recordings:
{    //    // IF true (default) recording audio and video is selected by default in the recording
dialog.    //    // recordAudioAndVideo:
true,    //    // If true, shows a notification at the start of the meeting with a call to action
button    //    // to start recording (for users who can do
so).    //    // suggestRecording:
```

```
true,    //    // If true, shows a warning label in the prejoin screen to point out the possibility
that    //    // the call you're joining might be
recorded.    //    // showPrejoinWarning:
true,    //    // If true, the notification for recording start will display a link to download the cloud
recording.    //    // showRecordingLink:
true,    //    // If true, mutes audio and video when a recording begins and displays a
dialog    //    // explaining the effect of
unmuting.    //    // requireConsent:
true,    //
},
// recordingService:
{    //     // When integrations like dropbox are enabled only that will be
shown,    //     // by enabling fileRecordingsServiceEnabled, we show both the
integrations    //     // and the generic recording service (its configuration and storage
type    //     // depends on jibri
configuration)    //     enabled:
false,
//     // Whether to show the possibility to share file recording with other
people    //     // (e.g. meeting participants), based on the actual
implementation    //     // on the
backend.    //     sharingEnabled:
false,
//     // Hide the warning that says we only store the recording for 24
hours.    //     hideStorageWarning:
false,    //
},
// DEPRECATED. Use recordingService.enabled
instead.    // fileRecordingsServiceEnabled:
false,
// DEPRECATED. Use recordingService.sharingEnabled
instead.    // fileRecordingsServiceSharingEnabled:
false,
// Local recording
configuration.    // localRecording:
{    //     // Whether to disable local recording or
not.    //     disable:
false,
//     // Whether to notify all participants when a participant is recording
locally.    //     notifyAllParticipants:
false,
//     // Whether to disable the self recording feature (only local participant
streams).    //     disableSelfRecording:
false,    //
},
// Customize the Live Streaming dialog. Can be modified for a non-YouTube
provider.    // liveStreaming:
{    //    // Whether to enable live streaming or
not.    //    enabled:
false,    //    // Terms
link    //    termsLink:
'https://www.youtube.com/t/terms',    //    // Data privacy
link    //    dataPrivacyLink:
'https://policies.google.com/privacy',    //    // RegExp string that validates the stream key input
field    //    validatorRegExpString:
'^(?:[a-zA-Z0-9]{4}(?:-(?!$)|$)){4}',    //    // Documentation reference for the live streaming
feature.    //    helpLink:
'https://jitsi.org/live'    //
},
// DEPRECATED. Use liveStreaming.enabled
instead.    // liveStreamingEnabled:
false,
// DEPRECATED. Use transcription.enabled
instead.    // transcribingEnabled:
false,
// DEPRECATED. Use transcription.useAppLanguage
instead.    // transcribeWithAppLanguage:
true,
// DEPRECATED. Use transcription.preferredLanguage
instead.    // preferredTranscribeLanguage:
'en-US',
// DEPRECATED. Use transcription.autoTranscribeOnRecord
instead.    // autoCaptionOnRecord:
false,
// Transcription
options.    // transcription:
{    //     // Whether the feature should be enabled or
not.    //     enabled:
false,
```

```
//     // Translation
languages.    //     // Available languages can be found
in    //     //
./lang/translation-languages.json.    //     translationLanguages: ['en', 'es', 'fr',
'ro'],
//     // Important languages to show on the top of the language
list.    //     translationLanguagesHead:
['en'],
//     // If true transcriber will use the application
language.    //     // The application language is either explicitly set by participants in their settings or
automatically    //     // detected based on the environment, e.g. if the app is opened in a chrome instance
which    //     // is using french as its default language then transcriptions for that participant will be in
french.    //     // Defaults to
true.    //     useAppLanguage:
true,
//     // Transcriber language. This settings will only work if
"useAppLanguage"    //     // is explicitly set to
false.    //     // Available languages can be found
in    //     //
./src/react/features/transcribing/transcriber-langs.json.    //     preferredLanguage:
'en-US',
//     // Enables automatic turning on transcribing when recording is
started    //     autoTranscribeOnRecord:
false,
//     // Enables automatic request of subtitles when transcriber is present in the meeting, uses the
default    //     // language that is
set    //     autoCaptionOnTranscribe:
false,    //
},
//
Misc
// Default value for the channel "last N" attribute. -1 for
unlimited.    channelLastN:
-1,
// Connection
indicators    // connectionIndicators:
{    //     autoHide:
true,    //     autoHideTimeout:
5000,    //     disabled:
false,    //     disableDetails:
false,    //     inactiveDisabled:
false    //
},
// Provides a way for the lastN value to be controlled through the
UI.    // When startLastN is present, conference starts with a last-n value of startLastN and
channelLastN    // value will be used when the quality level is selected using "Manage Video Quality"
slider.    // startLastN:
1,
// Specify the settings for video quality optimizations on the
client.    // videoQuality:
{
//    //    // Provides a way to set the codec preference on desktop based
endpoints.    //    codecPreferenceOrder: [ 'AV1', 'VP9', 'VP8', 'H264'
],
//    //    // Provides a way to set the codec for
screenshare.    //    screenshareCodec:
'AV1',    //    mobileScreenshareCodec:
'VP8',
//    //    // Enables the adaptive mode in the client that will make runtime adjustments to selected codecs and
received    //    // videos for a better user experience. This mode will kick in only when CPU overuse is reported in
the    //    // WebRTC statistics for the outbound video
streams.    //    enableAdaptiveMode:
false,
//    //    // Codec specific settings for scalability modes and max
bitrates.    //    av1:
{    //     maxBitratesVideo:
{    //         low:
100000,    //         standard:
300000,    //         high:
1000000,    //         fullHd:
2000000,    //         ultraHd:
4000000,    //         ssHigh:
2500000    //
},    //     scalabilityModeEnabled:
true,    //     useSimulcast:
false,    //     useKSVC:
true    //
},    //    h264:
```

```
{    //      maxBitratesVideo:
{    //          low:
200000,    //          standard:
500000,    //          high:
1500000,    //          fullHd:
3000000,    //          ultraHd:
6000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
true    //
},    //    vp8:
{    //      maxBitratesVideo:
{    //          low:
200000,    //          standard:
500000,    //          high:
1500000,    //          fullHd:
3000000,    //          ultraHd:
6000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
false    //
},    //    vp9:
{    //      maxBitratesVideo:
{    //          low:
100000,    //          standard:
300000,    //          high:
1200000,    //          fullHd:
2500000,    //          ultraHd:
5000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
true,    //      useSimulcast:
false,    //      useKSVC:
true    //
},
//    //    // The options can be used to override default thresholds of video thumbnail heights corresponding
to    //    // the video quality levels used in the application. At the time of this writing the allowed levels
are:    //    //     'low' - for the low quality level (180p at the time of this
writing)    //    //     'standard' - for the medium quality level
(360p)    //    //     'high' - for the high quality level
(720p)    //    // The keys should be positive numbers which represent the minimal thumbnail height for the quality
level.    //
//    //    // With the default config value below the application will use 'low' quality until the thumbnails
are    //    // at least 360 pixels tall. If the thumbnail height reaches 720 pixels then the application will switch
to    //    // the high
quality.    //    minHeightForQualityLvl:
{    //        360:
'standard',    //        720:
'high',    //
},
//    //    // Provides a way to set the codec preference
on mobile devices, both on RN and mobile browser based
endpoint    //    mobileCodecPreferenceOrder: [ 'VP8', 'VP9', 'H264', 'AV1'
],    //
},
// Notification
timeouts    // notificationTimeouts:
{    //      short:
2500,    //      medium:
5000,    //      long:
10000,    //      extraLong:
60000,    //
},
// // Options for the recording limit
notification.    // recordingLimit:
{
//    //    // The recording limit in minutes. Note: This number appears in the notification
text    //    // but doesn't enforce the actual recording time limit. This should be configured
in    //    //
jibri!    //    limit:
60,
//    //    // The name of the app with unlimited
recordings.    //    appName: 'Unlimited recordings
APP',
//    //    // The URL of the app with unlimited
recordings.    //    appURL:
'https://unlimited.recordings.app.com/',    //
},
```

```
// Disables or enables RTX (RFC 4588) (defaults to
false).    // disableRtx:
false,
// Moves all Jitsi Meet 'beforeunload' logic (cleanup, leaving, disconnecting, etc) to the 'unload'
event.    // disableBeforeUnloadHandlers:
true,
// Disables or enables TCC support in this client (default:
enabled).    // enableTcc:
true,
// Disables or enables REMB support in this client (default:
enabled).    // enableRemb:
true,
// Enables forced reload of the client when the call is migrated as a result
of    // the bridge going
down.    // enableForcedReload:
true,
// Use TURN/UDP servers for the jitsi-videobridge connection (by
default    // we filter out TURN/UDP because it is usually not needed since
the    // bridge itself is reachable via
UDP)    // useTurnUdp:
false
// Enable support for encoded transform in supported browsers. This
allows    // E2EE to work in Safari if the corresponding flag is enabled in the
browser.    //
Experimental.    // enableEncodedTransformSupport:
false,
//
UI
//
// Disables responsive
tiles.    // disableResponsiveTiles:
false,
// DEPRECATED. Please use `securityUi?.hideLobbyButton`
instead.    // Hides lobby
button.    // hideLobbyButton:
false,
// DEPRECATED. Please use `lobby?.autoKnock`
instead.    // If Lobby is enabled starts knocking
automatically.    // autoKnockLobby:
false,
// DEPRECATED. Please use `lobby?.enableChat`
instead.    // Enable lobby
chat.    // enableLobbyChat:
true,
// DEPRECATED! Use `breakoutRooms.hideAddRoomButton`
instead.    // Hides add breakout room
button    // hideAddRoomButton:
false,
// Require users to always specify a display
name.    // requireDisplayName:
true,
// Enables webhid functionality for
Audio.    // enableWebHIDFeature:
false,
// DEPRECATED! Use 'welcomePage.disabled'
instead.    // Whether to use a welcome page or not. In case it's false a random
room    // will be joined when no room is
specified.    // enableWelcomePage:
true,
// Configs for welcome
page.    // welcomePage:
{    //     // Whether to disable welcome page. In case it's disabled a random
room    //     // will be joined when no room is
specified.    //     disabled:
false,    //     // If set, landing page will redirect to this
URL.    //     customUrl:
''    //
},
// Configs for the lobby
screen.    // lobby:
{    //     // If Lobby is enabled, it starts knocking automatically. Replaces
`autoKnockLobby`.    //     autoKnock:
false,    //     // Enables the lobby chat. Replaces
`enableLobbyChat`.    //     enableChat:
true,    //
},
// Configs for the security related UI
elements.    // securityUi:
```

```
{    //     // Hides the lobby button. Replaces
`hideLobbyButton`.    //     hideLobbyButton:
false,    //     // Hides the possibility to set and enter a lobby
password.    //     disableLobbyPassword:
false,    //
},
// Disable app shortcuts that are registered upon joining a
conference    // disableShortcuts:
false,
// Disable initial browser getUserMedia
requests.    // This is useful for scenarios where users might want to start a conference for screensharing
only    // disableInitialGUM:
false,
// Enabling the close page will ignore the welcome page redirection
when    // a call is
hangup.    // enableClosePage:
false,
// Disable hiding of remote thumbnails when in a 1-on-1 conference
call.    // Setting this to null, will also disable showing the remote
videos    // when the toolbar is shown on mouse
movements    // disable1On1Mode: null | false |
true,
// Default local name to be
displayed    // defaultLocalDisplayName:
'me',
// Default remote name to be
displayed    // defaultRemoteDisplayName: 'Fellow
Jitster',
// Hides the display name from the participant
thumbnail    // hideDisplayName:
false,
// Hides the dominant speaker name badge that hovers above the
toolbox    // hideDominantSpeakerBadge:
false,
// Default language for the user interface. Cannot be
overwritten.    // DEPRECATED! Use the `lang` iframe option directly
instead.    // defaultLanguage:
'en',
// Disables profile and the edit of all fields from the profile settings (display name and
email)    // disableProfile:
false,
// Hides the email section under profile
settings.    // hideEmailInSettings:
false,
// When enabled the password used for locking a room is restricted to up to the number of digits
specified    // default: roomPasswordNumberOfDigits:
false,    // roomPasswordNumberOfDigits:
10,
// Message to show the users. Example: 'The service will be down
for    // maintenance at 01:00 AM
GMT,    // noticeMessage:
'',
// Enables calendar integration, depends on
googleApiApplicationClientID    // and
microsoftApiApplicationClientID    // enableCalendarIntegration:
false,
// Whether to notify when the conference is terminated because it was
destroyed.    // notifyOnConferenceDestruction:
true,
// The client id for the google APIs used for the calendar integration, youtube livestreaming,
etc.    // googleApiApplicationClientID:
'<client_id>',
// Configs for prejoin
page.    // prejoinConfig:
{    //     // When 'true', it shows an intermediate page before joining, where the user can configure their
devices.    //     // This replaces `prejoinPageEnabled`. Defaults to
true.    //     enabled:
true,    //     // Hides the participant name editing field in the prejoin
screen.    //     // If requireDisplayName is also set as true, a name should still be provided
through    //     // either the jwt or the userInfo from the iframe api init object in order for this to have an
effect.    //     hideDisplayName:
false,    //     // List of buttons to hide from the extra join options
dropdown.    //     hideExtraJoinButtons: ['no-audio',
'by-phone'],    //     // Configuration for pre-call
test    //     // By setting preCallTestEnabled, you enable the pre-call test in the prejoin
page.    //     // ICE server credentials need to be provided over the
preCallTestICEUrl    //     preCallTestEnabled:
false,    //     preCallTestICEUrl:
```

```
"    //
},
// When 'true', the user cannot edit the display
name.    // (Mainly useful when used in conjunction with the JWT so the JWT name becomes read
only.)    // readOnlyName:
false,
// If etherpad integration is enabled, setting this to true
will    // automatically open the etherpad when a participant joins.
This    // does not affect the mobile app since opening an
etherpad    // obscures the conference controls -- it's better to let
users    // choose to open the pad on their own in that
case.    // openSharedDocumentOnJoin:
false,
// If true, shows the unsafe room name warning label when a room name
is    // deemed unsafe (due to the simplicity in the name) and a password is
not    // set or the lobby is not
enabled.    // enableInsecureRoomNameWarning:
false,
// Array with avatar URL prefixes that need to use
CORS.    // corsAvatarURLs: [ 'https://www.gravatar.com/avatar/'
],
// Base URL for a Gravatar-compatible service. Defaults to
Gravatar.    // DEPRECATED! Use `gravatar.baseUrl`
instead.    // gravatarBaseURL:
'https://www.gravatar.com/avatar/',
// Setup for Gravatar-compatible
services.    // gravatar:
{    //    // Defaults to
Gravatar.    //    baseUrl:
'https://www.gravatar.com/avatar/',    //    // True if Gravatar should be
disabled.    //    disabled:
false,    //
},
// App name to be displayed in the invitation email subject, as an alternative
to    //
interfaceConfig.APP_NAME.    // inviteAppName:
null,
// Moved from
interfaceConfig(TOOLBAR_BUTTONS).    // The name of the toolbar buttons to display in the toolbar, including
the    // "More actions" menu. If present, the button will display. Exceptions
are    // "livestreaming" and "recording" which also require being a moderator
and    // some other values in config.js to be enabled. Also, the "profile" button
will    // not display for users with a
JWT.    //
Notes:    // - it's impossible to choose which buttons go in the "More actions"
menu    // - it's impossible to control the placement of
buttons    // - 'desktop' controls the "Share your screen"
button    // - if `toolbarButtons` is undefined, we fallback to enabling all buttons on the
UI    // toolbarButtons:
[    //
'camera',    //
'chat',    //
'closedcaptions',    //
'desktop',    //
'download',    //
'embedmeeting',    //
'etherpad',    //
'feedback',    //
'filmstrip',    //
'fullscreen',    //
'hangup',    //
'help',    //
'highlight',    //
'invite',    //
'linktosalesforce',    //
'livestreaming',    //
'microphone',    //
'noisesuppression',    //
'participants-pane',    //
'profile',    //
'raisehand',    //
'recording',    //
'security',    //
'select-background',    //
'settings',    //
'shareaudio',    //
'sharedvideo',    //
'shortcuts',    //
```

```
'stats',    //
'tileview',    //
'toggle-camera',    //
'videoquality',    //
'whiteboard',    //
],
// Holds values related to toolbar visibility
control.    // toolbarConfig:
{    //     // Moved from
interfaceConfig.INITIAL_TOOLBAR_TIMEOUT    //     // The initial number of milliseconds for the toolbar buttons to be visible on
screen.    //     initialTimeout:
20000,    //     // Moved from
interfaceConfig.TOOLBAR_TIMEOUT    //     // Number of milliseconds for the toolbar buttons to be visible on
screen.    //     timeout:
4000,    //     // Moved from
interfaceConfig.TOOLBAR_ALWAYS_VISIBLE    //     // Whether toolbar should be always visible or should hide after x
milliseconds.    //     alwaysVisible:
false,    //     // Indicates whether the toolbar should still autohide when chat is
open    //     autoHideWhileChatIsOpen:
false,    //
},
// Overrides the buttons displayed in the main toolbar. Depending on the screen size the number of
displayed    // buttons varies from 2 buttons to 8 buttons. Every array in the mainToolbarButtons array will replace
the    // corresponding default buttons configuration matched by the number of buttons specified in the array. Arrays
with    // more than 8 buttons or less then 2 buttons will be ignored. When there there isn't an override for a
certain    // configuration (for example when 3 buttons are displayed) the default jitsi-meet configuration will be
used.    // The order of the buttons in the array is
preserved.    // mainToolbarButtons:
[    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'reactions', 'participants-pane', 'tileview'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'participants-pane', 'tileview'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'participants-pane'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'participants-pane'
],    //     [ 'microphone', 'camera', 'chat', 'participants-pane'
],    //     [ 'microphone', 'camera', 'chat'
],    //     [ 'microphone', 'camera'
]    //
],
// Toolbar buttons which have their click/tap event exposed through the API
on    // `toolbarButtonClicked`. Passing a string for the button key
will    // prevent execution of the click/tap routine; passing an object with `key`
and    // `preventExecution` flag on false will not prevent execution of the
click/tap    // routine. Below array with mixed mode for passing the
buttons.    // buttonsWithNotifyClick:
[    //
'camera',    //
{    //         key:
'chat',    //         preventExecution:
false    //
},    //
{    //         key:
'closedcaptions',    //         preventExecution:
true    //
},    //
'desktop',    //
'download',    //
'embedmeeting',    //
'end-meeting',    //
'etherpad',    //
'feedback',    //
'filmstrip',    //
'fullscreen',    //
'hangup',    //
'hangup-menu',    //
'help',    //
{    //         key:
'invite',    //         preventExecution:
false    //
},    //
'livestreaming',    //
'microphone',    //
'mute-everyone',    //
'mute-video-everyone',    //
'noisesuppression',    //
'participants-pane',    //
'profile',    //
{    //         key:
'raisehand',    //         preventExecution:
true    //
```

```
},    //
'recording',    //
'security',    //
'select-background',    //
'settings',    //
'shareaudio',    //
'sharedvideo',    //
'shortcuts',    //
'stats',    //
'tileview',    //
'toggle-camera',    //
'videoquality',    //    // The add passcode button from the security
dialog.    //
{    //        key:
'add-passcode',    //        preventExecution:
false    //
},    //
'whiteboard',    //
],
// Participant context menu buttons which have their click/tap event exposed through the API
on    // `participantMenuButtonClick`. Passing a string for the button key
will    // prevent execution of the click/tap routine; passing an object with `key`
and    // `preventExecution` flag on false will not prevent execution of the
click/tap    // routine. Below array with mixed mode for passing the
buttons.    // participantMenuButtonsWithNotifyClick:
[    //
'allow-video',    //
{    //        key:
'ask-unmute',    //        preventExecution:
false    //
},    //
'conn-status',    //
'flip-local-video',    //
'grant-moderator',    //
{    //        key:
'kick',    //        preventExecution:
true    //
},    //
{    //        key:
'hide-self-view',    //        preventExecution:
false    //
},    //
'mute',    //
'mute-others',    //
'mute-others-video',    //
'mute-video',    //
'pinToStage',    //
'privateMessage',    //
{    //        key:
'remote-control',    //        preventExecution:
false    //
},    //
'send-participant-to-room',    //
'verify',    //
],
// List of pre meeting screens buttons to hide. The values must be one or more of the 5 allowed
buttons:    // 'microphone', 'camera', 'select-background', 'invite',
'settings'    // hiddenPremeetingButtons:
[],
// An array with custom option buttons for the participant context
menu    // type:  Array<{ icon: string; id: string; text: string;
}>    // customParticipantMenuButtons:
[],
// An array with custom option buttons for the
toolbar    // type:  Array<{ icon: string; id: string; text: string; backgroundColor?: string;
}>    // customToolbarButtons:
[],
//
Stats
//
// Whether to enable stats collection or not in the
TraceablePeerConnection.    // This can be useful for debugging purposes (post-processing/analysis
of    // the webrtc stats) as it is done in the jitsi-meet-torture
bandwidth    // estimation
tests.    // gatherStats:
false,
// The interval at which PeerConnection.getStats() is called. Defaults to
10000    // pcStatsInterval:
```

```
10000,
// Enables sending participants' display names to
stats    // enableDisplayNameInStats:
false,
// Enables sending participants' emails (if available) to stats and other
analytics    // enableEmailInStats:
false,
// faceLandmarks:
{    //     // Enables sharing your face coordinates. Used for centering faces within a
video.    //     enableFaceCentering:
false,
//     // Enables detecting face expressions and sharing data with other
participants    //     enableFaceExpressionsDetection:
false,
//     // Enables displaying face expressions in speaker
stats    //     enableDisplayFaceExpressions:
false,
//     // Enable rtc stats for face
landmarks    //     enableRTCStats:
false,
//     // Minimum required face movement percentage threshold for sending new face centering coordinates
data.    //     faceCenteringThreshold:
10,
//     // Milliseconds for processing a new image capture in order to detect face coordinates if they
exist.    //     captureInterval:
1000,    //
},
// Controls the percentage of automatic feedback shown to
participants.    // The default value is 100%. If set to 0, no automatic feedback will be
requested    // feedbackPercentage:
100,
//
Privacy
//
// If third party requests are disabled, no other server will be
contacted.    // This means avatars will be locally generated and external stats
integration    // will not
function.    // disableThirdPartyRequests:
false,

// Peer-To-Peer mode: used (if enabled) when there are just 2
participants.
//
p2p:
{        // Enables peer to peer mode. When enabled the system will try
to        // establish a direct connection when there are exactly 2
participants        // in the room. If that succeeds the conference will stop sending
data        // through the JVB and use the peer to peer connection instead. When
a        // 3rd participant joins the conference will be moved back to the
JVB        //
connection.        enabled:
true,
// Sets the ICE transport policy for the p2p connection. At the
time        // of this writing the list of possible values are 'all' and
'relay',        // but that is subject to change in the future. The enum is defined
in        // the WebRTC
standard:        //
https://www.w3.org/TR/webrtc/#rtcicetransportpolicy-enum.        // If not set, the effective value is
'all'.        // iceTransportPolicy:
'all',
// Provides a way to set the codec preference on mobile devices, both on RN and mobile browser
based        //
endpoints.        // mobileCodecPreferenceOrder: [ 'H264', 'VP8', 'VP9', 'AV1'
],
//        // Provides a way to set the codec preference on desktop based
endpoints.        // codecPreferenceOrder: [ 'AV1', 'VP9', 'VP8', 'H264
],
// Provides a way to set the codec for
screenshare.        // screenshareCodec:
'AV1',        // mobileScreenshareCodec:
'VP8',
// How long we're going to wait, before going back to P2P after the
3rd        // participant has left the conference (to filter out page
reload).        // backToP2PDelay:
5,
// The STUN servers that will be used in the peer to peer
connections        stunServers:
[
```

```
// { urls: 'stun:jitsi-gtw.inovamesh.cloud:3478'
},           { urls: 'stun:meet-jit-si-turnrelay.jitsi.net:443'
},
],
},
analytics:
{       // True if the analytics should be
disabled        // disabled:
false,
// Matomo
configuration:        // matomoEndpoint:
'https://your-matomo-endpoint/',        // matomoSiteID:
'42',
// The Amplitude APP
Key:        // amplitudeAPPKey:
'<APP_KEY>',
// Enables Amplitude UTM
tracking:        // Default value is
false.        // amplitudeIncludeUTM:
false,
// Obfuscates room name sent to analytics (amplitude,
rtcstats)        // Default value is
false.        // obfuscateRoomName:
false,
// Configuration for the rtcstats
server:        // By enabling rtcstats server every time a conference is joined the
rtcstats        // module connects to the provided rtcstatsEndpoint and sends statistics
regarding        // PeerConnection states along with getStats metrics polled at the
specified        //
interval.        // rtcstatsEnabled:
false,        // rtcstatsStoreLogs:
false,
// In order to enable rtcstats one needs to provide a endpoint
url.        // rtcstatsEndpoint:
wss://rtcstats-server-pilot.jitsi.net/,
// The interval at which rtcstats will poll getStats, defaults to
10000ms.        // If the value is set to 0 getStats won't be polled and the rtcstats
client        // will only send data related to RTCPeerConnection
events.        // rtcstatsPollInterval:
10000,
// This determines if rtcstats sends the SDP to the rtcstats server or
replaces        // all SDPs with an empty string
instead.        // rtcstatsSendSdp:
false,
// Array of script URLs to load as lib-jitsi-meet "analytics
handlers".        // scriptURLs:
[       //
"https://example.com/my-custom-analytics.js",        //
],
// By enabling watchRTCEnabled option you would want to use watchRTC
feature        // This would also require to configure
watchRTCConfigParams.        // Please remember to keep rtcstatsEnabled disabled for watchRTC to
work.        // watchRTCEnabled:
false,
},
// Logs that should go be passed through the 'log' event if a handler is defined for
it    // apiLogLevels: ['warn', 'log', 'error', 'info',
'debug'],
// Information about the jitsi-meet instance we are connecting to,
including    // the user region as seen by the
server.    // deploymentInfo:
{    //     shard:
"shard1",    //     region:
"europe",    //     userRegion:
"asia",    //
},
// Array<string> of disabled
sounds.    // Possible
values:    // -
'ASKED_TO_UNMUTE_SOUND'    // -
'E2EE_OFF_SOUND'    // -
'E2EE_ON_SOUND'    // -
'INCOMING_MSG_SOUND'    // -
'KNOCKING_PARTICIPANT_SOUND'    // -
'LIVE_STREAMING_OFF_SOUND'    // -
'LIVE_STREAMING_ON_SOUND'    // -
'NO_AUDIO_SIGNAL_SOUND'    // -
'NOISY_AUDIO_INPUT_SOUND'    // -
```

```
'OUTGOING_CALL_EXPIRED_SOUND'    // -
'OUTGOING_CALL_REJECTED_SOUND'    // -
'OUTGOING_CALL_RINGING_SOUND'    // -
'OUTGOING_CALL_START_SOUND'    // -
'PARTICIPANT_JOINED_SOUND'    // -
'PARTICIPANT_LEFT_SOUND'    // -
'RAISE_HAND_SOUND'    // -
'REACTION_SOUND'    // -
'RECORDING_OFF_SOUND'    // -
'RECORDING_ON_SOUND'    // -
'TALK_WHILE_MUTED_SOUND'    // disabledSounds:
[],
// DEPRECATED! Use `disabledSounds`
instead.    // Decides whether the start/stop recording audio notifications should play on
record.    // disableRecordAudioNotification:
false,
// DEPRECATED! Use `disabledSounds`
instead.    // Disables the sounds that play when other participants join or leave
the    // conference (if set to true, these sounds will not be
played).    // disableJoinLeaveSounds:
false,
// DEPRECATED! Use `disabledSounds`
instead.    // Disables the sounds that play when a chat message is
received.    // disableIncomingMessageSound:
false,
// Information for the chrome extension
banner    // chromeExtensionBanner:
{    //    // The chrome extension to be installed
address    //    url:
'https://chrome.google.com/webstore/detail/jitsi-meetings/kglhbbefdnlheedjiejgomgmfplipfeb',    //    edgeUrl:
'https://microsoftedge.microsoft.com/addons/detail/jitsi-meetings/eeecajlpbgjppibfledfihobcabccihn',
//    // Extensions info which allows checking if they are installed or
not    //    chromeExtensionsInfo:
[    //
{    //            id:
'kglhbbefdnlheedjiejgomgmfplipfeb',    //            path:
'jitsi-logo-48x48.png',    //
},    //        // Edge extension
info    //
{    //            id:
'eeecajlpbgjppibfledfihobcabccihn',    //            path:
'jitsi-logo-48x48.png',    //
},    //
]    //
},
// e2ee:
{    //    labels:
{    //    description:
'',    //    label:
'',    //    tooltip:
'',    //    warning:
'',    //
},    //    externallyManagedKey:
false,    //    disabled:
false,    //
},
// Options related to end-to-end (participant to participant)
ping.    // e2eping:
{    //    // Whether ene-to-end pings should be
enabled.    //    enabled:
false,
//    //    // The number of responses to wait
for.    //    numRequests:
5,
//    //    // The max conference size in which e2e pings will be
sent.    //    maxConferenceSize:
200,
//    //    // The maximum number of e2e ping messages per second for the whole conference to aim
for.    //    // This is used to control the pacing of messages in order to reduce the load on the
backend.    //    maxMessagesPerSecond:
250,    //
},
// If set, will attempt to use the provided video input device label
when    // triggering a screenshare, instead of proceeding through the normal
flow    // for obtaining a desktop
stream.    // NOTE: This option is experimental and is currently intended for
internal    // use
only.    // _desktopSharingSourceDevice:
```

```
'sample-id-or-label',
// DEPRECATED! Use deeplinking.disabled
instead.    // If true, any checks to handoff to another application will be
prevented    // and instead the app will continue to display in the current
browser.    // disableDeepLinking:
false,
// The deeplinking
config.    // For information about the properties
of    // deeplinking.[ios/android].dynamicLink
check:    //
https://firebase.google.com/docs/dynamic-links/create-manually    // deeplinking:
{
//    //     // The desktop deeplinking config, disabled by
default.    //     desktop:
{    //         appName: 'Jitsi
Meet',    //         appScheme:
'jitsi-meet,    //         download:
{    //
linux:    //
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet-x86_64.AppImage',    //             macos:
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet.dmg',    //             windows:
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet.exe'    //
},    //         enabled:
false    //
},    //     // If true, any checks to handoff to another application will be
prevented    //     // and instead the app will continue to display in the current
browser.    //     disabled:
false,
//     // whether to hide the logo on the deep linking
pages.    //     hideLogo:
false,
//     // The ios deeplinking
config.    //     ios:
{    //         appName: 'Jitsi
Meet',    //         // Specify mobile app scheme for opening the app from the mobile
browser.    //         appScheme:
'org.jitsi.meet',    //         // Custom URL for downloading ios mobile
app.    //         downloadLink:
'https://itunes.apple.com/us/app/jitsi-meet/id1165103905',    //         dynamicLink:
{    //             apn:
'org.jitsi.meet',    //             appCode:
'w2atb',    //             customDomain:
undefined,    //             ibi:
'com.atlassian.JitsiMeet.ios',    //             isi:
'1165103905'    //
}    //
},
//     // The android deeplinking
config.    //     android:
{    //         appName: 'Jitsi
Meet',    //         // Specify mobile app scheme for opening the app from the mobile
browser.    //         appScheme:
'org.jitsi.meet',    //         // Custom URL for downloading android mobile
app.    //         downloadLink:
'https://play.google.com/store/apps/details?id=org.jitsi.meet',    //         // Android app package
name.    //         appPackage:
'org.jitsi.meet',    //         fDroidUrl:
'https://f-droid.org/en/packages/org.jitsi.meet/',    //         dynamicLink:
{    //             apn:
'org.jitsi.meet',    //             appCode:
'w2atb',    //             customDomain:
undefined,    //             ibi:
'com.atlassian.JitsiMeet.ios',    //             isi:
'1165103905'    //
}    //
}    //
},
// // The terms, privacy and help centre
URL's.    // legalUrls:
{    //     helpCentre:
'https://web-cdn.jitsi.net/faq/meet-faq.html',    //     privacy:
'https://jitsi.org/meet/privacy',    //     terms:
'https://jitsi.org/meet/terms'    //
},
// A property to disable the right click context menu for
localVideo    // the menu has option to flip the locally seen video for local
presentations    // disableLocalVideoFlip:
false,
```

```
// A property used to unset the default flip state of the local
video.    // When it is set to 'true', the local(self) video will not be mirrored
anymore.    // doNotFlipLocalVideo:
false,
// Mainly privacy related
settings
// Disables all invite functions from the app (share, invite, dial
out...etc)    // disableInviteFunctions:
true,
// Disables storing the room name to the recents list. When in an iframe this is ignored
and    // the room is never stored in the recents
list.    // doNotStoreRoom:
true,
// Deployment specific
URLs.    // deploymentUrls:
{    //    // If specified a 'Help' button will be displayed in the overflow menu with a link to the specified URL
for    //    // user
documentation.    //    userDocumentationURL:
'https://docs.example.com/video-meetings.html',    //    // If specified a 'Download our apps' button will be displayed in the overflow menu with a
link    //    // to the specified URL for an app download
page.    //    downloadAppsUrl:
'https://docs.example.com/our-apps.html',    //
},
// Options related to the remote participant
menu.    // remoteVideoMenu:
{    //     // Whether the remote video context menu to be rendered or
not.    //     disabled:
true,    //     // If set to true the 'Switch to visitor' button will be
disabled.    //     disableDemote:
true,    //     // If set to true the 'Kick out' button will be
disabled.    //     disableKick:
true,    //     // If set to true the 'Grant moderator' button will be
disabled.    //     disableGrantModerator:
true,    //     // If set to true the 'Send private message' button will be
disabled.    //     disablePrivateChat:
true,    //
},
// Endpoint that enables support for salesforce integration with in-meeting resource
linking    // This is required
for:    // listing the most recent records -
salesforceUrl/records/recents    // searching records -
salesforceUrl/records?text=${text}    // retrieving record details -
salesforceUrl/records/${id}?type=${type}    // and linking the meeting -
salesforceUrl/sessions/${sessionId}/records/${id}
//    // salesforceUrl:
'https://api.example.com/',
// If set to true all muting operations of remote participants will be
disabled.    // disableRemoteMute:
true,

/**     External API url used to receive branding specific
information.     If there is no url set or there are missing fields, the defaults are
applied.     The config file should be in
JSON.     None of the fields are mandatory and the response must have the
shape:
{       // Whether participant can only send group chat message if `send-groupchat` feature is enabled in
jwt.       groupChatRequiresPermission:
false,       // Whether participant can only create polls if `create-polls` feature is enabled in
jwt.       pollCreationRequiresPermission:
false,       // The domain url to apply (will replace the domain in the sharing conference link/embed
section)       inviteDomain:
'example-company.org',       // The hex value for the colour used as
background       backgroundColor:
'#fff',       // The url for the image used as
background       backgroundImageUrl:
'https://example.com/background-img.png',       // The anchor url used when clicking the logo
image       logoClickUrl:
'https://example-company.org',       // The url used for the image used as
logo       logoImageUrl:
'https://example.com/logo-img.png',       // Overwrite for pool of background images for
avatars       avatarBackgrounds: ['url(https://example.com/avatar-background-1.png)',
'#FFF'],       // The lobby/prejoin screen
background       premeetingBackground:
'url(https://example.com/premeeting-background.png)',       // A list of images that can be used as video
backgrounds.       // When this field is present, the default images will be replaced with those
provided.       virtualBackgrounds:
['https://example.com/img.jpg'],       // Object containing customized icons that should replace the default
ones.
```

```
// The keys need to be the exact same icon names used in
here:        //
https://github.com/jitsi/jitsi-meet/blob/master/react/features/base/icons/svg/index.ts        // To avoid having the icons trimmed or displayed in an
unexpected way, please provide
svg        // files containing svg xml icons in the size that the default icons come
in.        customIcons:
{            IconArrowUp:
'https://example.com/arrow-up.svg',            IconDownload:
'https://example.com/download.svg',            IconRemoteControlStart:
'https://example.com/remote-start.svg',
},        // Object containing a theme's properties. It also supports partial overwrites of the main
theme.        // For a list of all possible theme tokens and their current defaults, please
check:        //
https://github.com/jitsi/jitsi-meet/tree/master/resources/custom-theme/custom-theme.json        // For a short explanations on each of the tokens,
please
check:        //
https://github.com/jitsi/jitsi-meet/blob/master/react/features/base/ui/Tokens.ts        // IMPORTANT!: This is work in progress so many of the various
tokens are not yet applied in
code        // or they are partially
applied.        customTheme:
{            palette:
{                ui01: "orange
!important",                ui02:
"maroon",                surface02:
'darkgreen',                ui03:
"violet",                ui04:
"magenta",                ui05:
"blueviolet",                action01:
'green',                action01Hover:
'lightgreen',                disabled01:
'beige',                success02:
'cadetblue',                action02Hover:
'aliceblue',
},            typography:
{                labelRegular:
{                    fontSize:
25,                    lineHeight:
30,                    fontWeight:
500,
}
}
}
}
*/    // dynamicBrandingUrl:
'',
// A list of allowed URL domains for shared
video.
//    //
NOTE:    // '*' is allowed value and it will allow any URL to be used for shared video. We do not recommend using
'*',    // use it at your own
risk!    // sharedVideoAllowedURLDomains: [
],
// Options related to the participants
pane.    // participantsPane:
{    //    // Enables
feature    //    enabled:
true,    //    // Hides the moderator settings
tab.    //    hideModeratorSettingsTab:
false,    //    // Hides the more actions
button.    //    hideMoreActionsButton:
false,    //    // Hides the mute all
button.    //    hideMuteAllButton:
false,    //
},
// Options related to the breakout rooms
feature.    // breakoutRooms:
{    //    // Hides the add breakout room button. This replaces
`hideAddRoomButton`.    //    hideAddRoomButton:
false,    //    // Hides the auto assign participants
button.    //    hideAutoAssignButton:
false,    //    // Hides the join breakout room
button.    //    hideJoinRoomButton:
false,    //
},
// When true, virtual background feature will be
disabled.    // disableVirtualBackground:
false,
// When true the user cannot add more images to be used as virtual
```

```
background.    // Only the default ones from will be
available.    // disableAddingBackgroundImages:
false,
// Sets the background transparency level. '0' is fully transparent, '1' is
opaque.    // backgroundAlpha:
1,
// The URL of the moderated rooms microservice, if available. If
it    // is present, a link to the service will be rendered on the welcome
page,    // otherwise the app doesn't render
it.    // moderatedRoomServiceUrl:
'https://moderated.jitsi-gtw.inovamesh.cloud',
// If true, tile view will not be enabled automatically when the participants count threshold is
reached.    // disableTileView:
true,
// If true, the tiles will be displayed contained within the available space rather than enlarged to cover
it,    // with a 16:9 aspect ratio (old
behaviour).    // disableTileEnlargement:
true,
// Controls the visibility and behavior of the top header conference info
labels.    // If a label's id is not in any of the 2 arrays, it will not be visible at all on the
header.    // conferenceInfo:
{    //     // those labels will not be hidden in tandem with the
toolbox.    //     alwaysVisible: ['recording',
'raised-hands-count'],    //     // those labels will be auto-hidden in tandem with the toolbox
buttons.    //     autoHide:
[    //
'subject',    //
'conference-timer',    //
'participants-count',    //
'e2ee',    //
'video-quality',    //
'insecure-room',    //
'highlight-moment',    //
'top-panel-toggle',    //
]    //
},
// Hides the conference
subject    // hideConferenceSubject:
false,
// Hides the conference
timer.    // hideConferenceTimer:
false,
// Hides the recording
label    // hideRecordingLabel:
false,
// Hides the participants
stats    // hideParticipantsStats:
true,
// Sets the conference
subject    // subject: 'Conference
Subject',
// Sets the conference local
subject    // localSubject: 'Conference Local
Subject',
// This property is related to the use case when jitsi-meet is used via the IFrame API. When the property is
true    // jitsi-meet will use the local storage of the host page instead of its own. This option is useful if the
browser    // is not persisting the local storage inside the
iframe.    // useHostPageLocalStorage:
true,
// Etherpad ("shared document")
integration.
//    // If set, add a "Open shared document" link to the bottom right menu
that    // will open an etherpad
document.    // etherpad_base:
'https://your-etherpad-installati.on/p/',
// To enable information about dial-in access to meetings you need to
provide    // dialInNumbersUrl and
dialInConfCodeUrl.    // dialInNumbersUrl returns a json array of numbers that can be used for
dial-in.    // {"countryCode":"US","tollFree":false,"formattedNumber":"+1
123-456-7890"}    // dialInConfCodeUrl is the conference mapper converting a meeting id to a PIN used for
dial-in    // or the other way around (more info in
resources/cloud-api.swagger)
// You can use external service for authentication that will redirect back passing a jwt
token    // You can use tokenAuthUrl config to point to a URL of such
service.    // The URL for the service supports few params which will be filled in by the
code.    //
tokenAuthUrl:    //
'https://myservice.com/auth/{room}?code_challenge_method=S256&code_challenge={code_challenge}&state={state}'    // Supported parameters in
```

```
tokenAuthUrl:    //      {room} - will be replaced with the room
name    //      {code_challenge} - (A web only). A oauth 2.0 code challenge that will be sent to the service.
See:    //          https://datatracker.ietf.org/doc/html/rfc7636. The code verifier will be saved in the
sessionStorage    //          under key:
'code_verifier'.    //      {state} - A json with the current state before redirecting. Keys that are included in the
state:    //          - room (The current room name as shown in the address
bar)    //          - roomSafe (the backend safe room name to use (lowercase), that is passed to the
backend)    //          - tenant (The tenant if
any)    //          - config.xxx (all config
overrides)    //          - interfaceConfig.xxx (all interfaceConfig
overrides)    //          - ios=true (in case ios mobile app is
used)    //          - android=true (in case android mobile app is
used)    //          - electron=true (when web is loaded in electron
app)    // If there is a logout service you can specify its URL
with:    // tokenLogoutUrl:
'https://myservice.com/logout'    // You can enable tokenAuthUrlAutoRedirect which will detect that you have logged in successfully
before    // and will automatically redirect to the token service to get the token for the
meeting.    // tokenAuthUrlAutoRedirect:
false    // An option to respect the context.tenant jwt field compared to the current tenant from the
url    // tokenRespectTenant:
false,
// You can put an array of values to target different entity types in the invite
dialog.    // Valid values are "phone", "room", "sip", "user", "videosipgw" and
"email"    // peopleSearchQueryTypes: ["user",
"email"],    // Directory endpoint which is called for invite dialog
autocomplete    // peopleSearchUrl:
"https://myservice.com/api/people",    // Endpoint which is called to send invitation
requests    // inviteServiceUrl:
"https://myservice.com/api/invite",
// For external entities (e. g. email), the localStorage key holding the token value for directory
authentication    // peopleSearchTokenLocation:
"mytoken",

// Options related to
visitors.    // visitors:
{    //     // Starts audio/video when the participant is promoted from
visitor.    //     enableMediaOnPromote:
{    //         audio:
true,    //         video:
true    //
},    //
},    // The default type of desktop sharing sources that will be used in the electron
app.    // desktopSharingSources: ['screen',
'window'],
// Disables the echo cancelation for local audio
tracks.    // disableAEC:
true,
// Disables the auto gain control for local audio
tracks.    // disableAGC:
true,
// Disables the audio processing (echo cancelation, auto gain control and noise suppression) for local audio
tracks.    // disableAP:
true,
// Disables the anoise suppression for local audio
tracks.    // disableNS:
true,
// Replaces the display name with the JID of the
participants.    // displayJids:
true,
// Enables disables talk while muted
detection.    // enableTalkWhileMuted:
true,
// Sets the peer connection ICE transport policy to
"relay".    // forceTurnRelay:
true,
// List of undocumented settings used in
jitsi-meet
/**
_immediateReloadThreshold
deploymentInfo
dialOutAuthUrl
dialOutCodesUrl
dialOutRegionUrl
disableRemoteControl
iAmRecorder
iAmSipGateway
microsoftApiApplicationClientID
*/
```

```
/**     * This property can be used to alter the generated meeting invite links (in combination with a branding
domain     * which is retrieved internally by jitsi meet) (e.g.
https://meet.jit.si/someMeeting     * can become
https://brandedDomain/roomAlias)
*/    // brandingRoomAlias:
null,
// List of undocumented settings used in
lib-jitsi-meet
/**
_peerConnStatusOutOfLastNTimeout
_peerConnStatusRtcMuteTimeout
avgRtpStatsN
desktopSharingSources
disableLocalStats
hiddenDomain
hiddenFromRecorderFeatureEnabled
ignoreStartMuted
websocketKeepAlive
websocketKeepAliveUrl
*/

/**     * Default interval (milliseconds) for triggering mouseMoved iframe API
event
*/    mouseMoveCallbackInterval:
1000,

/**       Use this array to configure which notifications will be shown to the
user       The items correspond to the title or description key of that
notification       Some of these notifications also depend on some other internal logic to be displayed or
not,       so adding them here will not ensure they will always be
displayed
A falsy value for this prop will result in having all notifications enabled (e.g null, undefined,
false)
*/    // notifications:
[    //     'connection.CONNFAIL', // shown when the connection
fails,    //     'dialog.cameraConstraintFailedError', // shown when the camera
failed    //     'dialog.cameraNotSendingData', // shown when there's no feed from user's
camera    //     'dialog.kickTitle', // shown when user has been
kicked    //     'dialog.liveStreaming', // livestreaming notifications (pending, on, off,
limits)    //     'dialog.lockTitle', // shown when setting conference password
fails    //     'dialog.maxUsersLimitReached', // shown when maximmum users limit has been
reached    //     'dialog.micNotSendingData', // shown when user's mic is not sending any
audio    //     'dialog.passwordNotSupportedTitle', // shown when setting conference password fails due to password
format    //     'dialog.recording', // recording notifications (pending, on, off,
limits)    //     'dialog.remoteControlTitle', // remote control notifications (allowed, denied, start, stop,
error)    //
'dialog.reservationError',    //     'dialog.screenSharingFailedTitle', // shown when the screen sharing
failed    //     'dialog.serviceUnavailable', // shown when server is not
reachable    //     'dialog.sessTerminated', // shown when there is a failed conference
session    //     'dialog.sessionRestarted', // show when a client reload is initiated because of bridge
migration    //     'dialog.tokenAuthFailed', // show when an invalid jwt is
used    //     'dialog.tokenAuthFailedWithReasons', // show when an invalid jwt is used with the reason behind the
error    //     'dialog.transcribing', // transcribing notifications (pending,
off)    //     'dialOut.statusMessage', // shown when dial out status is
updated.    //     'liveStreaming.busy', // shown when livestreaming service is
busy    //     'liveStreaming.failedToStart', // shown when livestreaming fails to
start    //     'liveStreaming.unavailableTitle', // shown when livestreaming service is not
reachable    //     'lobby.joinRejectedMessage', // shown when while in a lobby, user's request to join is
rejected    //     'lobby.notificationTitle', // shown when lobby is toggled and when join requests are allowed /
denied    //     'notify.audioUnmuteBlockedTitle', // shown when mic unmute
blocked    //     'notify.chatMessages', // shown when receiving chat messages while the chat window is
closed    //     'notify.connectedOneMember', // show when a participant
joined    //     'notify.connectedThreePlusMembers', // show when more than 2 participants joined
simultaneously    //     'notify.connectedTwoMembers', // show when two participants joined
simultaneously    //     'notify.dataChannelClosed', // shown when the bridge channel has been
disconnected    //     'notify.hostAskedUnmute', // shown to participant when host asks them to
unmute    //     'notify.invitedOneMember', // shown when 1 participant has been
invited    //     'notify.invitedThreePlusMembers', // shown when 3+ participants have been
invited    //     'notify.invitedTwoMembers', // shown when 2 participants have been
invited    //     'notify.kickParticipant', // shown when a participant is
kicked    //     'notify.leftOneMember', // show when a participant
left    //     'notify.leftThreePlusMembers', // show when more than 2 participants left
simultaneously    //     'notify.leftTwoMembers', // show when two participants left
simultaneously    //     'notify.linkToSalesforce', // shown when joining a meeting with salesforce
integration    //     'notify.localRecordingStarted', // shown when the local recording has been
started    //     'notify.localRecordingStopped', // shown when the local recording has been
stopped    //     'notify.moderationInEffectCSTitle', // shown when user attempts to share content during AV
```

```
moderation    //     'notify.moderationInEffectTitle', // shown when user attempts to unmute audio during AV
moderation    //     'notify.moderationInEffectVideoTitle', // shown when user attempts to enable video during AV
moderation    //     'notify.moderator', // shown when user gets moderator
privilege    //     'notify.mutedRemotelyTitle', // shown when user is muted by a remote
party    //     'notify.mutedTitle', // shown when user has been muted upon
joining,    //     'notify.newDeviceAudioTitle', // prompts the user to use a newly detected audio
device    //     'notify.newDeviceCameraTitle', // prompts the user to use a newly detected
camera    //     'notify.noiseSuppressionFailedTitle', // shown when failed to start noise
suppression    //     'notify.participantWantsToJoin', // shown when lobby is enabled and participant requests to join
meeting    //     'notify.participantsWantToJoin', // shown when lobby is enabled and participants request to join
meeting    //     'notify.passwordRemovedRemotely', // shown when a password has been removed
remotely    //     'notify.passwordSetRemotely', // shown when a password has been set
remotely    //     'notify.raisedHand', // shown when a participant used raise
hand,    //     'notify.screenShareNoAudio', // shown when the audio could not be shared for the selected
screen    //     'notify.screenSharingAudioOnlyTitle', // shown when the best performance has been affected by screen
sharing    //     'notify.selfViewTitle', // show "You can always un-hide the self-view from
settings"    //     'notify.startSilentTitle', // shown when user joined with no
audio    //     'notify.suboptimalExperienceTitle', // show the browser
warning    //     'notify.unmute', // shown to moderator when user raises hand during AV
moderation    //     'notify.videoMutedRemotelyTitle', // shown when user's video is muted by a remote
party,    //     'notify.videoUnmuteBlockedTitle', // shown when camera unmute and desktop sharing are
blocked    //
'prejoin.errorDialOut',    //
'prejoin.errorDialOutDisconnected',    //
'prejoin.errorDialOutFailed',    //
'prejoin.errorDialOutStatus',    //
'prejoin.errorStatusCode',    //
'prejoin.errorValidation',    //     'recording.busy', // shown when recording service is
busy    //     'recording.failedToStart', // shown when recording fails to
start    //     'recording.unavailableTitle', // shown when recording service is not
reachable    //     'toolbar.noAudioSignalTitle', // shown when a broken mic is
detected    //     'toolbar.noisyAudioInputTitle', // shown when noise is detected for the current
microphone    //     'toolbar.talkWhileMutedPopup', // shown when user tries to speak while
muted    //     'transcribing.failed', // shown when transcribing
fails    //
],
// List of notifications to be disabled. Works in tandem with the above
setting.    // disabledNotifications:
[],
// Prevent the filmstrip from autohiding when screen width is under a certain
threshold    // disableFilmstripAutohiding:
false,
// filmstrip:
{    //     // Disable the vertical/horizontal
filmstrip.    //     disabled:
false,    //     // Disables user resizable filmstrip. Also, allows configuration of the
filmstrip    //     // (width, tiles aspect ratios) through the interfaceConfig
options.    //     disableResizable:
false,
//     // Disables the stage
filmstrip    //     // (displaying multiple participants on stage besides the vertical
filmstrip)    //     disableStageFilmstrip:
false,
//     // Default number of participants that can be displayed on
stage.    //     // The user can change this in settings. Number must be between 1 and
6.    //     stageFilmstripParticipants:
1,
//     // Disables the top panel (only shown when a user is sharing their
screen).    //     disableTopPanel:
false,
//     // The minimum number of participants that must be in the call
for    //     // the top panel layout to be
used.    //     minParticipantCountForTopPanel:
50,    //
},
// Tile view related config
options.    // tileView:
{    //     // Whether tileview should be
disabled.    //     disabled:
false,    //     // The optimal number of tiles that are going to be shown in tile view. Depending on the screen size it
may    //     // not be possible to show the exact number of participants specified
here.    //     numberOfVisibleTiles:
25,    //
},
// Specifies whether the chat emoticons are disabled or
not    // disableChatSmileys:
false,
// Settings for the GIPHY
```

```
integration.    // giphy:
{    //     // Whether the feature is enabled or
not.    //     enabled:
false,    //     // SDK API Key from
Giphy.    //     sdkKey:
'',    //     // Display mode can be one
of:    //     // - tile: show the GIF on the tile of the participant that sent
it.    //     // - chat: show the GIF as a message in
chat    //     // - all: all of the above. This is the default
option    //     displayMode:
'all',    //     // How long the GIF should be displayed on the tile (in
milliseconds).    //     tileTime:
5000,    //     // Limit results by rating: g, pg, pg-13, r. Default value:
g.    //     rating:
'pg',    //
},
//
Logging    // logging:
{    //     // Default log level for the app and
lib-jitsi-meet.    //     defaultLogLevel:
'trace',    //     // Option to disable
LogCollector.    //     //disableLogCollector:
true,    //     // Individual loggers are
customizable.    //     loggers:
{    //         // The following are too verbose in their logging with the default
level.    //         'modules/RTC/TraceablePeerConnection.js':
'info',    //         'modules/xmpp/strophe.util.js':
'log',    //
},    //
},
// Application logo
url    // defaultLogoUrl:
'images/watermark.svg',
// Settings for the Excalidraw whiteboard
integration.    // whiteboard:
{    //     // Whether the feature is enabled or
not.    //     enabled:
true,    //     // The server used to support whiteboard
collaboration.    //     //
https://github.com/jitsi/excalidraw-backend    //     collabServerBaseUrl:
'https://excalidraw-backend.example.com',    //     // The user access limit to the whiteboard, introduced as a
means    //     // to control the
performance.    //     userLimit:
25,    //     // The url for more info about the whiteboard and its usage
limitations.    //     limitUrl:
'https://example.com/blog/whiteboard-limits',    //
},
// The watchRTC initialize config params as described
:    //
https://testrtc.com/docs/installing-the-watchrtc-javascript-sdk/#h-set-up-the-sdk    //
https://www.npmjs.com/package/@testrtc/watchrtc-sdk    // watchRTCConfigParams:
{    //         /** Watchrtc api key
*/    //         rtcApiKey:
string;    //         /** Identifier for the session
*/    //         rtcRoomId?:
string;    //         /** Identifier for the current peer
*/    //         rtcPeerId?:
string;    //
/**    //          * ["tag1", "tag2",
"tag3"]    //          * @deprecated use 'keys'
instead    //
*/    //         rtcTags?:
string[];    //         /** { "key1": "value1", "key2": "value2"}
*/    //         keys?:
any;    //         /** Enables additional logging
*/    //         debug?:
boolean;    //         rtcToken?:
string;    //
/**    //          * @deprecated No longer needed. Use "proxyUrl"
instead.    //
*/    //         wsUrl?:
string;    //         proxyUrl?:
string;    //         console?:
{    //             level:
string;    //             override:
boolean;    //
};    //         allowBrowserLogCollection?:
boolean;    //         collectionInterval?:
```

```
number;    //         logGetStats?:
boolean;    //
},
// Hide login button on auth dialog, you may want to enable this if you are using JWT tokens to authenticate
users    // hideLoginButton:
true,
// If true remove the tint foreground on focused user camera in
filmstrip    // disableCameraTintForeground:
false,};

// Set the default values for JaaS
customersif (enableJaaS)
{    config.dialInNumbersUrl =
'https://conference-mapper.jitsi.net/v1/access/dids';    config.dialInConfCodeUrl =
'https://conference-mapper.jitsi.net/v1/access';    config.roomPasswordNumberOfDigits = 10; // skip re-adding it (do not remove
comment)}
</script><!-- adapt to your needs, i.e. set hosts and bosh path
-->    <script>/* eslint-disable no-unused-vars, no-var, max-len
*//* eslint sort-keys: ["error", "asc", {"caseSensitive": false}]
*/
/**
*
!!!IMPORTANT!!!
* * This file is considered deprecated. All options will eventually be moved
to * config.js, and no new options should be added
here.
*/
var interfaceConfig =
{    APP_NAME: 'Jitsi
Meet',    AUDIO_LEVEL_PRIMARY_COLOR:
'rgba(255,255,255,0.4)',    AUDIO_LEVEL_SECONDARY_COLOR:
'rgba(255,255,255,0.2)',

/**     * A UX mode where the last screen share participant is
automatically     * pinned. Valid values are the string "remote-only" so remote
participants     * get pinned but not local, otherwise any truthy value for all
participants,     * and any falsy value to disable the
feature.
*     * Note: this mode is experimental and subject to
breakage.
*/    AUTO_PIN_LATEST_SCREEN_SHARE:
'remote-only',    BRAND_WATERMARK_LINK:
'',
CLOSE_PAGE_GUEST_HINT: false, // A html text to be shown to guests on the close page, false disables
it
DEFAULT_BACKGROUND:
'#040404',    DEFAULT_WELCOME_PAGE_LOGO_URL:
'images/watermark.svg',
DISABLE_DOMINANT_SPEAKER_INDICATOR:
false,

/**     * If true, notifications regarding joining/leaving are no longer
displayed.
*/    DISABLE_JOIN_LEAVE_NOTIFICATIONS:
false,

/**     * If true, presence status: busy, calling, connected etc. is not
displayed.
*/    DISABLE_PRESENCE_STATUS:
false,

/**     * Whether the speech to text transcription subtitles panel is
disabled.     * If {@code undefined}, defaults to {@code
false}.
*     * @type
{boolean}
*/    DISABLE_TRANSCRIPTION_SUBTITLES:
false,

/**     * Whether or not the blurred video background for large video should
be     * displayed on browsers that can support
it.
*/    DISABLE_VIDEO_BACKGROUND:
false,
DISPLAY_WELCOME_FOOTER:
true,    DISPLAY_WELCOME_PAGE_ADDITIONAL_CARD:
false,    DISPLAY_WELCOME_PAGE_CONTENT:
false,    DISPLAY_WELCOME_PAGE_TOOLBAR_ADDITIONAL_CONTENT:
```

```
false,
ENABLE_DIAL_OUT:
true,
FILM_STRIP_MAX_HEIGHT:
120,
GENERATE_ROOMNAMES_ON_WELCOME_PAGE:
true,

/**     * Hide the invite prompt in the header when alone in the
meeting.
*/    HIDE_INVITE_MORE_HEADER:
false,
JITSI_WATERMARK_LINK:
'https://jitsi.org',
LANG_DETECTION: true, // Allow i18n to detect the system
language    LOCAL_THUMBNAIL_RATIO: 16 / 9, //
16:9

/**     * Maximum coefficient of the ratio of the large video to the visible
area     * after the large video is scaled to fit the
window.
*     * @type
{number}
*/    MAXIMUM_ZOOMING_COEFFICIENT:
1.3,

/**     * Whether the mobile app Jitsi Meet is to be promoted to
participants     * attempting to join a conference in a mobile Web browser.
If     * {@code undefined}, defaults to {@code
true}.
*     * @type
{boolean}
*/    MOBILE_APP_PROMO:
true,
// Names of browsers which should show a warning stating the current
browser    // has a suboptimal experience. Browsers which are not listed as optimal
or    // unsupported are considered suboptimal. Valid values
are:    // chrome, chromium, electron, firefox , safari,
webkit    OPTIMAL_BROWSERS: [ 'chrome', 'chromium', 'firefox', 'electron', 'safari', 'webkit'
],
POLICY_LOGO:
null,    PROVIDER_NAME:
'Jitsi',

/**     * If true, will display recent
list
*     * @type
{boolean}
*/    RECENT_LIST_ENABLED:
true,    REMOTE_THUMBNAIL_RATIO: 1, //
1:1
SETTINGS_SECTIONS: [ 'devices', 'language', 'moderator', 'profile', 'calendar', 'sounds', 'more'
],

/**     * Specify which sharing features should be displayed. If the value is not
set     * all sharing features will be shown. You can set [] to disable
all.
*/    // SHARING_FEATURES: ['email', 'url', 'dial-in',
'embed'],
SHOW_BRAND_WATERMARK:
false,

/**     * Decides whether the chrome extension banner should be rendered on the landing page and during the
meeting.     * If this is set to false, the banner will not be rendered at all. If set to true, the check for
extension(s)     * being already installed is done before
rendering.
*/    SHOW_CHROME_EXTENSION_BANNER:
false,
SHOW_JITSI_WATERMARK:
true,    SHOW_POWERED_BY:
false,    SHOW_PROMOTIONAL_CLOSE_PAGE:
false,

/*     * If indicated some of the error dialogs may point to the support URL
for     *
help.
*/    SUPPORT_URL:
'https://community.jitsi.org/',
```

```
// Browsers, in addition to those which do not fully support WebRTC,
that    // are not supported and should show the unsupported browser
page.    UNSUPPORTED_BROWSERS:
[],

/**     * Whether to show thumbnails in filmstrip as a column instead of as a
row.
*/    VERTICAL_FILMSTRIP:
true,
// Determines how the video would fit the screen. 'both' would fit the
whole    // screen, 'height' would fit the original video height to the height of
the    // screen, 'width' would fit the original video width to the width of
the    // screen respecting ratio, 'nocrop' would make the video as large
as    // possible and preserve aspect ratio without
cropping.    VIDEO_LAYOUT_FIT:
'both',

/**     * If true, hides the video quality label indicating the resolution
status     * of the current large
video.
*     * @type
{boolean}
*/    VIDEO_QUALITY_LABEL_DISABLED:
false,

/**     * How many columns the tile view can expand to. The respected range
is     * between 1 and
5.
*/    // TILE_VIEW_MAX_COLUMNS:
5,
// List of undocumented
settings
/**
INDICATOR_FONT_SIZES
PHONE_NUMBER_REGEX
*/
// -----------------DEPRECATED CONFIGS BELOW THIS
LINE-----------------------------

/**     * Specify URL for downloading ios mobile
app.
*/    // MOBILE_DOWNLOAD_LINK_IOS:
'https://itunes.apple.com/us/app/jitsi-meet/id1165103905',

/**     * Specify custom URL for downloading android mobile
app.
*/    // MOBILE_DOWNLOAD_LINK_ANDROID:
'https://play.google.com/store/apps/details?id=org.jitsi.meet',

/**     * Specify mobile app scheme for opening the app from the mobile
browser.
*/    // APP_SCHEME:
'org.jitsi.meet',
// NATIVE_APP_NAME: 'Jitsi
Meet',

/**     * Specify Firebase dynamic link properties for the mobile
apps.
*/    // MOBILE_DYNAMIC_LINK:
{    //    APN:
'org.jitsi.meet',    //    APP_CODE:
'w2atb',    //    CUSTOM_DOMAIN:
undefined,    //    IBI:
'com.atlassian.JitsiMeet.ios',    //    ISI:
'1165103905'    //
},

/**     * Hide the logo on the deep linking
pages.
*/    // HIDE_DEEP_LINKING_LOGO:
false,

/**     * Specify the Android app package
name.
*/    // ANDROID_APP_PACKAGE:
'org.jitsi.meet',

/**     * Specify custom URL for downloading f droid
```

```
app.
*/    // MOBILE_DOWNLOAD_LINK_F_DROID:
'https://f-droid.org/packages/org.jitsi.meet/',
// Connection indicators
(    //
CONNECTION_INDICATOR_AUTO_HIDE_ENABLED,    //
CONNECTION_INDICATOR_AUTO_HIDE_TIMEOUT,    // CONNECTION_INDICATOR_DISABLED) got moved to
config.js.
// Please use disableModeratorIndicator from
config.js    // DISABLE_FOCUS_INDICATOR:
false,
// Please use defaultLocalDisplayName from
config.js    // DEFAULT_LOCAL_DISPLAY_NAME:
'me',
// Please use defaultLogoUrl from
config.js    // DEFAULT_LOGO_URL:
'images/watermark.svg',
// Please use defaultRemoteDisplayName from
config.js    // DEFAULT_REMOTE_DISPLAY_NAME: 'Fellow
Jitster',
// Moved to config.js as
`toolbarConfig.initialTimeout`.    // INITIAL_TOOLBAR_TIMEOUT:
20000,
// Please use `liveStreaming.helpLink` from
config.js    // Documentation reference for the live streaming
feature.    // LIVE_STREAMING_HELP_LINK:
'https://jitsi.org/live',
// Moved to config.js as
`toolbarConfig.alwaysVisible`.    // TOOLBAR_ALWAYS_VISIBLE:
false,
// This config was moved to config.js as
`toolbarButtons`.    // TOOLBAR_BUTTONS:
[],
// Moved to config.js as
`toolbarConfig.timeout`.    // TOOLBAR_TIMEOUT:
4000,
// Allow all above example options to include a trailing comma
and    // prevent fear when commenting out the last
value.    // eslint-disable-next-line
sort-keys    makeJsonParserHappy: 'even if last key had a trailing
comma'
// No configuration value should follow this
line.};

/* eslint-enable no-unused-vars, no-var, max-len
*/</script>
<script
src="libs/lib-jitsi-meet.min.js?v=8542"></script>    <script
src="libs/app.bundle.min.js?v=8542"></script>    <title>Jitsi
Meet</title><meta property="og:title" content="Jitsi
Meet"/><meta property="og:image"
content="images/jitsilogo.png?v=1"/><meta property="og:description" content="Join a WebRTC video conference powered by the Jitsi
Videobridge"/><meta description="Join a WebRTC video conference powered by the Jitsi
Videobridge"/><meta itemprop="name" content="Jitsi
Meet"/><meta itemprop="description"
content="Join a WebRTC video conference powered by the Jitsi
Videobridge"/><meta itemprop="image"
content="images/jitsilogo.png?v=1"/><link rel="icon"
href="images/favicon.svg?v=1">
<template id =
"welcome-page-additional-content-template"></template>
<template id =
"welcome-page-additional-card-template"></template>
<template
id="settings-toolbar-additional-content-template"></template>

</head>
<body>    <noscript
aria-hidden="true">        <div>JavaScript is disabled. </br>For this site to work you have to enable
JavaScript.</div>
</noscript>
<div id="react"
role="main"></div>
</body></html>
-CR-
```

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /
HTTP/1.1Host:
jitsi-gtw.inovamesh.cloudConnection:
Keep-Alive

HTTP/1.1 200
OKServer: nginx/1.24.0
(Ubuntu)Date: Tue, 01 Jul 2025 20:17:09
GMTContent-Type:
text/htmlTransfer-Encoding:
chunkedConnection:
keep-aliveVary:
Accept-EncodingStrict-Transport-Security:
max-age=63072000
<html itemscope itemtype="http://schema.org/Product" prefix="og: http://ogp.me/ns#"
xmlns="http://www.w3.org/1999/html">
<head>
<meta
charset="utf-8"> <meta http-equiv="content-type"
content="text/html;charset=utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0,
maximum-scale=1.0"> <meta name="theme-color"
content="#2A3A4B"> <base href="/"
/>

<link rel="apple-touch-icon"
href="images/apple-touch-icon.png"> <link rel="stylesheet"
href="css/all.css?v=8542">
<link rel="manifest"
id="manifest-placeholder">

<script> function contextRoot(pathname)
{ const contextRootEndIndex =
pathname.lastIndexOf('/');

```
return
(               contextRootEndIndex ===
-1              ?
'/'             : pathname.substring(0, contextRootEndIndex +
1)
);
}       window.EXCALIDRAW_ASSET_PATH =
'libs/';        // Dynamically generate the manifest location URL. It must be served from the document origin, and we may
have        // the base pointing to the CDN. This way we can generate a full URL which will bypass the
base.       document.querySelector('#manifest-placeholder').setAttribute('href', window.location.origin + contextRoot(window.location.pathname) +
'manifest.json');
document.addEventListener('DOMContentLoaded', () =>
{           if (!JitsiMeetJS.app)
{
return;
}

JitsiMeetJS.app.renderEntryPoint({              Component:
JitsiMeetJS.app.entryPoints.APP
})
const isEmbedded = () =>
{               try
{                   return window.self !==
window.top;             } catch (e)
{                   return
true;
}
};
const isElectron =
navigator.userAgent.includes('Electron');           const shouldRegisterWorker = !isElectron && !isEmbedded() && 'serviceWorker' in
navigator;
if (shouldRegisterWorker)
{
navigator.serviceWorker                 .register(window.location.origin + contextRoot(window.location.pathname) +
'pwa-worker.js')                .then(reg =>
{                       console.log('Service worker registered.',
reg);
})                  .catch(err =>
{
console.log(err);
});
}
});
</script>
<script>        // IE11 and earlier can be identified via their user agent and
be        // redirected to a page that is known to have no newer js
syntax.       if (window.navigator.userAgent.match(/(MSIE|Trident)/))
{           var roomName =
encodeURIComponent(window.location.pathname);           window.location.pathname =
'static/recommendedBrowsers.html';
}
window.indexLoadedTime =
window.performance.now();       console.log("(TIME) index.html loaded:\t",
indexLoadedTime);       window.addEventListener('load', function()
{           window.loadedEventTime =
window.performance.now();           console.log("(TIME) window loaded event:\t",
loadedEventTime);
});
// XXX the code below listeners for errors and displays an error
message        // in the document body when any of the required files fails to
load.       // The intention is to prevent from displaying broken
page.       var criticalFiles =
[
"config.js",
"utils.js",
"do_external_connect.js",
"interface_config.js",
"lib-jitsi-meet.min.js",
"app.bundle.min.js",
"all.css?v=8542"
];      var loadErrHandler = function(e)
{           var target =
e.target;           // Error on <script> and
<link>(CSS)           // <script> will have .src and <link>
.href           var fileRef = (target.src ? target.src :
target.href);           if (("SCRIPT" === target.tagName || "LINK" ===
target.tagName)             &&
criticalFiles.some(                 function(file) { return fileRef.indexOf(file) !== -1 }))
```

```
{               window.onload = function()
{                   // The whole complex part below implements page reloads
with                    // "exponential backoff". The retry attempt is passes
as                  // "rCounter" query
parameter                   var href =
window.location.href;
var retryMatch =
href.match(/.+(\?|&)rCounter=(\d+)/);                   var retryCountStr = retryMatch ? retryMatch[2] :
"0";                    var retryCount =
Number.parseInt(retryCountStr);
if (retryMatch == null)
{                       var separator = href.indexOf("?") === -1 ? "?" :
"&";                        var hashIdx =
href.indexOf("#");
if (hashIdx === -1)
{                           href += separator +
"rCounter=1";                       } else
{                           var hashPart =
href.substr(hashIdx);
href = href.substr(0,
hashIdx)                                + separator + "rCounter=1" +
hashPart;
}                   } else
{                       var separator =
retryMatch[1];
href =
href.replace(
/(\?|&)rCounter=(\d+)/,                          separator + "rCounter=" + (retryCount +
1));
}
var delay = Math.pow(2, retryCount) *
2000;                   if (isNaN(delay) || delay < 2000 || delay >
60000)                      delay =
10000;
var showMoreText = "show
more";                  var showLessText = "show
less";

document.body.innerHTML                         = "<div
style='"                        + "position: absolute;top: 50%;left:
50%;"                       + "text-align:
center;"                        + "font-size:
medium;"                        + "font-weight:
400;"                       + "transform: translate(-50%,
-50%)'>"                        + "Uh oh! We couldn't fully download everything we needed
:("                     + "<br/>
"                       + "We will try again shortly. In the mean time, check for problems with your Internet
connection!"                        + "<br/><br/>
"                   + "<div id='moreInfo'
style='"                        + "display: none;'>" + "Missing " +
fileRef                     +
"<br/><br/></div>"                          + "<a id='showMore'
style='"                        + "text-decoration:
underline;"                         +
"font-size:small;"                          + "cursor: pointer'>" + showMoreText +
"</a>"                      +
""                      + "<a id ='reloadLink'
style='"                        + "text-decoration:
underline;"                         +
"font-size:small;"                          + "'>reload
now</a>"                        +
"</div>";
var reloadLink =
document.getElementById('reloadLink');                  reloadLink.setAttribute('href',
href);
var showMoreElem =
document.getElementById("showMore");                    showMoreElem.addEventListener('click', function ()
{                       var
moreInfoElem                                =
document.getElementById("moreInfo");
if (showMoreElem.innerHTML === showMoreText)
{
moreInfoElem.setAttribute(
"style",                                "display:
block;"                                 +
"color:#FF991F;"                                +
"font-size:small;"                              +
"user-select:text;");                           showMoreElem.innerHTML =
```

```
showLessText;
}                       else
{
moreInfoElem.setAttribute(                              "style", "display:
none;");                        showMoreElem.innerHTML =
showMoreText;
}
});

window.setTimeout(                      function () { window.location.replace(href); },
delay);
// Call extra handler if
defined.                if (typeof postLoadErrorHandler === "function")
{
postLoadErrorHandler(fileRef);
}
};
window.removeEventListener(                 'error', loadErrHandler, true /* capture phase
*/);
}
};
window.addEventListener(            'error', loadErrHandler, true /* capture phase type of listener
*/);
</script>    <script>/* eslint-disable comma-dangle, no-unused-vars, no-var, prefer-template, vars-on-top
*/
/*
* NOTE: If you add a new option please remember to document it
here: *
https://jitsi.github.io/handbook/docs/dev-guide/dev-guide-configuration
*/
var subdir =
';var subdomain =
';
if (subdomain)
{    subdomain = subdomain.substr(0, subdomain.length -
1).split('.')
.join('_')        .toLowerCase() +
'.';}

// In case of no ssi provided by the webserver, use empty
stringsif (subdir.startsWith('<!--'))
{    subdir =
';}
if (subdomain.startsWith('<!--'))
{    subdomain =
';}

var enableJaaS =
false;
var config =
{    //
Connection
//
hosts:
{        // XMPP
domain.        domain:
'jitsi-gtw.inovamesh.cloud',
// When using authentication, domain for guest
users.        // anonymousdomain:
'guest.example.com',
// Domain for authenticated users. Defaults to
<domain>.        // authdomain:
'jitsi-gtw.inovamesh.cloud',
// Focus component domain. Defaults to
focus.<domain>.        // focus:
'focus.jitsi-gtw.inovamesh.cloud',
// XMPP MUC domain. FIXME: use XEP-0030 to discover
it.        muc: 'conference.' + subdomain +
'jitsi-gtw.inovamesh.cloud',
},
// BOSH URL. FIXME: use XEP-0156 to discover
it.    bosh: 'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'http-bind',
// Websocket URL
(XMPP)    websocket: 'wss://jitsi-gtw.inovamesh.cloud/' + subdir +
'xmpp-websocket',
// websocketKeepAliveUrl: 'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'_unlock',
```

```
// Whether BOSH should be preferred over WebSocket if both are
configured.    // preferBosh:
false,
// The real JID of focus participant - can be overridden
here    // Do not change username - FIXME: Make focus username
configurable    //
https://github.com/jitsi/jitsi-meet/issues/7376    // focusUserJid:
'focus@auth.jitsi-gtw.inovamesh.cloud',
// Option to send conference requests to jicofo over http (requires nginx rule for
it)    //
conferenceRequestUrl:    //    'https://jitsi-gtw.inovamesh.cloud/' + subdir +
'conference-request/v1',
// Options related to the bridge (colibri) data
channel    bridgeChannel:
{        // If the backend advertises multiple colibri websockets, this options
allows        // to filter some of them out based on the domain name. We use the first
URL        // which does not match ignoreDomain, falling back to the first one that
matches        // ignoreDomain. Has no effect if
undefined.        // ignoreDomain:
'example.com',
// Prefer SCTP (WebRTC data channels over the media path) over a colibri
websocket.        // If SCTP is available in the backend it will be used instead of a WS. Defaults
to        // false (SCTP is used only if available and no WS are
available).        // preferSctp:
false
},
// Testing / experimental
features.
//
testing:
{        // Allows the setting of a custom bandwidth value from the
UI.        // assumeBandwidth:
true,
// Enables use of getDisplayMedia in
electron        // electronUseGetDisplayMedia:
false,
// Enables the use of the codec selection API supported by the browsers
.        // enableCodecSelectionAPI:
false,
// P2P test mode disables automatic switching to P2P when there are
2        // participants in the
conference.        // p2pTestMode:
false,
// Enables the test specific features consumed by
jitsi-meet-torture        // testMode:
false,
// Disables the auto-play behavior of *all* newly created video
element.        // This is useful when the client runs on a host with limited
resources.        // noAutoPlayVideo:
false,
// Experiment: Whether to skip interim
transcriptions.        // skipInterimTranscriptions:
false,
// Dump transcripts to a <transcript> element for
debugging.        // dumpTranscript:
false,
// Log the audio
levels.        // debugAudioLevels:
true,
// Will replace ice candidates IPs with invalid ones in order to fail
ice.        // failICE:
true,
},
// Disables moderator
indicators.    // disableModeratorIndicator:
false,
// Disables the reactions
feature.    // disableReactions:
true,
// Disables the reactions moderation
feature.    // disableReactionsModeration:
false,
// Disables polls
feature.    // disablePolls:
false,
// Disables demote button from
self-view    // disableSelfDemote:
false,
```

```
// Disables self-view tile. (hides it from tile view and from
filmstrip)    // disableSelfView:
false,
// Disables self-view settings in
UI    // disableSelfViewSettings:
false,
// screenshotCapture :
{    //      Enables the screensharing capture
feature.    //      enabled:
false,
//    //      The mode for the screenshot capture
feature.    //      Can be either 'recording' - screensharing screenshots are
taken    //      only when the recording is also
on,    //      or 'always' - screensharing screenshots are always
taken.    //      mode:
'recording',    //
}
// Disables ICE/UDP by filtering out local and remote UDP candidates
in    //
signalling.    // webrtcIceUdpDisable:
false,
// Disables ICE/TCP by filtering out local and remote TCP candidates
in    //
signalling.    // webrtcIceTcpDisable:
false,

//
Media
//
//
Audio
// Disable measuring of audio
levels.    // disableAudioLevels:
false,
// audioLevelsInterval:
200,
// Enabling this will run the lib-jitsi-meet no audio detection module
which    // will notify the user if the current selected microphone has no
audio    // input and will suggest another valid device if one is
present.    enableNoAudioDetection:
true,
// Enabling this will show a "Save Logs" link in the GSM popover that can
be    // used to collect debug information (XMPP IQs, SDP offer/answer
cycles)    // about the
call.    // enableSaveLogs:
false,
// Enabling this will hide the "Show More" link in the GSM popover that can
be    // used to display more statistics about the connection (IP, Port, protocol,
etc).    // disableShowMoreStats:
true,
// Enabling this will run the lib-jitsi-meet noise detection module which
will    // notify the user if there is noise, other than voice, coming from the
current    // selected microphone. The purpose it to let the user know that the input
could    // be potentially unpleasant for other meeting
participants.    enableNoisyMicDetection:
true,
// Start the conference in audio only mode (no video is being received
nor    //
sent).    // startAudioOnly:
false,
// Every participant after the Nth will start audio
muted.    // startAudioMuted:
10,
// Start calls with audio muted. Unlike the option above, this one is
only    // applied locally. FIXME: having these 2 options is
confusing.    // startWithAudioMuted:
false,
// Enabling it (with #params) will disable local audio output of
remote    // participants and to enable it back a reload is
needed.    // startSilent:
false,
// Enables support for opus-red (redundancy for
Opus).    // enableOpusRed:
false,
// Specify audio quality stereo and opusMaxAverageBitrate values in order to enable HD
audio.    // Beware, by doing so, you are disabling echo cancellation, noise suppression and
AGC.    // Specify enableOpusDtx to enable support for opus-dtx
where    // audio packets wont be transmitted while participant is silent or
```

```
muted.    // audioQuality:
{    //     stereo:
false,    //     opusMaxAverageBitrate: null, // Value to fit the 6000 to 510000
range.    //     enableOpusDtx:
false,    //
},
// Noise suppression configuration. By default rnnoise is used. Optionally
Krisp    // can be used by enabling it below, but the Krisp JS SDK files must be supplied in
your    // installation. Specifically, these files are
needed:    //   -
https://meet.example.com/libs/krisp/krisp.mjs    //   -
https://meet.example.com/libs/krisp/models/model_8.kw    //   -
https://meet.example.com/libs/krisp/models/model_nc.kw    //   -
https://meet.example.com/libs/krisp/models/model_bvc.kw    //   -
https://meet.example.com/libs/krisp/assets/bvc-allowed.txt    //     In case when you have known BVC supported devices and you want to extend
allowed devices
list    //   -
https://meet.example.com/libs/krisp/assets/bvc-allowed-ext.txt    //     In case when you have known BVC supported devices and you want to extend
allowed devices
list    //   -
https://meet.example.com/libs/krisp/models/model_inbound_8.kw    //   -
https://meet.example.com/libs/krisp/models/model_inbound_16.kw    //     In case when you want to use inbound noise suppression
models    // NOTE: Krisp JS SDK v2.0.0 was
tested.    // noiseSuppression:
{    //     krisp:
{    //         enabled:
false,    //         logProcessStats:
false,    //         debugLogs:
false,    //         useBVC:
false,    //         bufferOverflowMS:
1000,    //         inboundModels:
{    //             modelInbound8:
'model_inbound_8.kef',    //             modelInbound16:
'model_inbound_16.kef',    //
},    //         preloadInboundModels:
{    //             modelInbound8:
'model_inbound_8.kef',    //             modelInbound16:
'model_inbound_16.kef',    //
},    //         preloadModels:
{    //             modelBVC:
'model_bvc.kef',    //             model8:
'model_8.kef',    //             modelNC:
'model_nc_mq.kef',    //
},    //         models:
{    //             modelBVC:
'model_bvc.kef',    //             model8:
'model_8.kef',    //             modelNV:
'model_nc_mq.kef',    //
},    //         bvc:
{    //             allowedDevices:
'bvc-allowed.txt',    //             allowedDevicesExt:
'bvc-allowed-ext.txt',    //
}    //
},    //
},
//
Video
// Sets the default camera facing
mode.    // cameraFacingMode:
'user',
// Sets the preferred resolution (height) for local video. Defaults to
720.    // resolution:
720,
// DEPRECATED. Please use raisedHands.disableRemoveRaisedHandOnFocus
instead.    // Specifies whether the raised hand will hide when someone becomes a dominant speaker or
not    // disableRemoveRaisedHandOnFocus:
false,
// Specifies which raised hand related config should be
set.    // raisedHands:
{    //     // Specifies whether the raised hand can be lowered by
moderator.    //     disableLowerHandByModerator:
false,
//     // Specifies whether there is a notification before hiding the raised
hand    //     // when someone becomes the dominant
speaker.    //     disableLowerHandNotification:
true,
//     // Specifies whether there is a notification when you are the next speaker in
line.    //     disableNextSpeakerNotification:
```

```
false,
//     // Specifies whether the raised hand will hide when someone becomes a dominant speaker or
not.    //     disableRemoveRaisedHandOnFocus:
false,    //
},
// speakerStats:
{    //     // Specifies whether the speaker stats is enable or
not.    //     disabled:
false,
//     // Specifies whether there will be a search field in speaker stats or
not.    //     disableSearch:
false,
//     // Specifies whether participants in speaker stats should be ordered or not, and with what
priority.    //     // 'role', <- Moderators on
top.    //     // 'name', <- Alphabetically by
name.    //     // 'hasLeft', <- The ones that have left in the
bottom.    //     order:
[    //
'role',    //
'name',    //
'hasLeft',    //
],    //
},
// DEPRECATED. Please use speakerStats.disableSearch
instead.    // Specifies whether there will be a search field in speaker stats or
not    // disableSpeakerStatsSearch:
false,
// DEPRECATED. Please use speakerStats.order
.    // Specifies whether participants in speaker stats should be ordered or not, and with what
priority    // speakerStatsOrder:
[    //  'role', <- Moderators on
top    //  'name', <- Alphabetically by
name    //  'hasLeft', <- The ones that have left in the
bottom    // ], <- the order of the array elements determines
priority
// How many participants while in the tile view mode, before the receiving video quality is reduced from HD to
SD.    // Use -1 to
disable.    // maxFullResolutionParticipants:
2,
// w3c spec-compliant video constraints to use for video capture.
Currently    // used by browsers that return true from
lib-jitsi-meet's    // util#browser#usesNewGumFlow. The constraints are independent
from    // this config's resolution value. Defaults to requesting an
ideal    // resolution of
720p.    // constraints:
{    //     video:
{    //         height:
{    //             ideal:
720,    //             max:
720,    //             min:
240,    //
},    //
},    //
},
// Enable / disable simulcast
support.    // disableSimulcast:
false,
// Every participant after the Nth will start video
muted.    // startVideoMuted:
10,
// Start calls with video muted. Unlike the option above, this one is
only    // applied locally. FIXME: having these 2 options is
confusing.    // startWithVideoMuted:
false,
// Desktop
sharing
// Optional desktop sharing frame rate options. Default value: min:5,
max:5.    // desktopSharingFrameRate:
{    //     min:
5,    //     max:
5,    //
},
// Optional screenshare settings that give more control over screen capture in the
browser.    // screenShareSettings:
{    //     // Show users the current tab is the preferred capture source, default:
false.    //     desktopPreferCurrentTab:
false,    //     // Allow users to select system audio, default:
include.    //     desktopSystemAudio:
```

```
'include',    //      // Allow users to seamlessly switch which tab they are sharing without having to select the tab
again.    //      desktopSurfaceSwitching:
'include',    //      // Allow a user to be shown a preference for what screen is to be captured, default:
unset.    //      desktopDisplaySurface:
undefined,    //      // Allow users to select the current tab as a capture source, default:
exclude.    //      desktopSelfBrowserSurface:
'exclude'    //
},
//
Recording
// Enable the dropbox
integration.    // dropbox:
{    //      appKey: '<APP_KEY>', // Specify your app key
here.    //      // A URL to redirect the user to, after
authenticating    //      // by default
uses:    //      //
'https://jitsi-gtw.inovamesh.cloud/static/oauth.html'    //
redirectURI:    //
'https://jitsi-gtw.inovamesh.cloud/subfolder/static/oauth.html',    //
},
// configuration for all things recording related. Existing settings will be migrated here in the
future.    // recordings:
{    //    // IF true (default) recording audio and video is selected by default in the recording
dialog.    //    // recordAudioAndVideo:
true,    //    // If true, shows a notification at the start of the meeting with a call to action
button    //    // to start recording (for users who can do
so).    //    // suggestRecording:
true,    //    // If true, shows a warning label in the prejoin screen to point out the possibility
that    //    // the call you're joining might be
recorded.    //    // showPrejoinWarning:
true,    //    // If true, the notification for recording start will display a link to download the cloud
recording.    //    // showRecordingLink:
true,    //    // If true, mutes audio and video when a recording begins and displays a
dialog    //    // explaining the effect of
unmuting.    //    // requireConsent:
true,    //
},
// recordingService:
{    //      // When integrations like dropbox are enabled only that will be
shown,    //      // by enabling fileRecordingsServiceEnabled, we show both the
integrations    //      // and the generic recording service (its configuration and storage
type    //      // depends on jibri
configuration)    //      enabled:
false,
//      // Whether to show the possibility to share file recording with other
people    //      // (e.g. meeting participants), based on the actual
implementation    //      // on the
backend.    //      sharingEnabled:
false,
//      // Hide the warning that says we only store the recording for 24
hours.    //      hideStorageWarning:
false,    //
},
// DEPRECATED. Use recordingService.enabled
instead.    // fileRecordingsServiceEnabled:
false,
// DEPRECATED. Use recordingService.sharingEnabled
instead.    // fileRecordingsServiceSharingEnabled:
false,
// Local recording
configuration.    // localRecording:
{    //      // Whether to disable local recording or
not.    //      disable:
false,
//      // Whether to notify all participants when a participant is recording
locally.    //      notifyAllParticipants:
false,
//      // Whether to disable the self recording feature (only local participant
streams).    //      disableSelfRecording:
false,    //
},
// Customize the Live Streaming dialog. Can be modified for a non-YouTube
provider.    // liveStreaming:
{    //    // Whether to enable live streaming or
not.    //    enabled:
false,    //    // Terms
link    //    termsLink:
'https://www.youtube.com/t/terms',    //    // Data privacy
```

```
link    //    dataPrivacyLink:
'https://policies.google.com/privacy',    //    // RegExp string that validates the stream key input
field    //    validatorRegExpString:
'^(?:[a-zA-Z0-9]{4}(?:-(?!$)|$)){4}',    //    // Documentation reference for the live streaming
feature.    //    helpLink:
'https://jitsi.org/live'    //
},
// DEPRECATED. Use liveStreaming.enabled
instead.    // liveStreamingEnabled:
false,
// DEPRECATED. Use transcription.enabled
instead.    // transcribingEnabled:
false,
// DEPRECATED. Use transcription.useAppLanguage
instead.    // transcribeWithAppLanguage:
true,
// DEPRECATED. Use transcription.preferredLanguage
instead.    // preferredTranscribeLanguage:
'en-US',
// DEPRECATED. Use transcription.autoTranscribeOnRecord
instead.    // autoCaptionOnRecord:
false,
// Transcription
options.    // transcription:
{    //    // Whether the feature should be enabled or
not.    //    enabled:
false,
//    // Translation
languages.    //    // Available languages can be found
in    //    //
./lang/translation-languages.json.    //    translationLanguages: ['en', 'es', 'fr',
'ro'],
//    // Important languages to show on the top of the language
list.    //    translationLanguagesHead:
['en'],
//    // If true transcriber will use the application
language.    //    // The application language is either explicitly set by participants in their settings or
automatically    //    // detected based on the environment, e.g. if the app is opened in a chrome instance
which    //    // is using french as its default language then transcriptions for that participant will be in
french.    //    // Defaults to
true.    //    useAppLanguage:
true,
//    // Transcriber language. This settings will only work if
"useAppLanguage"    //    // is explicitly set to
false.    //    // Available languages can be found
in    //    //
./src/react/features/transcribing/transcriber-langs.json.    //    preferredLanguage:
'en-US',
//    // Enables automatic turning on transcribing when recording is
started    //    autoTranscribeOnRecord:
false,
//    // Enables automatic request of subtitles when transcriber is present in the meeting, uses the
default    //    // language that is
set    //    autoCaptionOnTranscribe:
false,    //
},
//
Misc
// Default value for the channel "last N" attribute. -1 for
unlimited.    channelLastN:
-1,
// Connection
indicators    // connectionIndicators:
{    //    autoHide:
true,    //    autoHideTimeout:
5000,    //    disabled:
false,    //    disableDetails:
false,    //    inactiveDisabled:
false    //
},
// Provides a way for the lastN value to be controlled through the
UI.    // When startLastN is present, conference starts with a last-n value of startLastN and
channelLastN    // value will be used when the quality level is selected using "Manage Video Quality"
slider.    // startLastN:
1,
// Specify the settings for video quality optimizations on the
client.    // videoQuality:
{
```

```
//    //    // Provides a way to set the codec preference on desktop based
endpoints.    //    codecPreferenceOrder: [ 'AV1', 'VP9', 'VP8', 'H264'
],
//    //    // Provides a way to set the codec for
screenshare.    //    screenshareCodec:
'AV1',    //    mobileScreenshareCodec:
'VP8',
//    //    // Enables the adaptive mode in the client that will make runtime adjustments to selected codecs and
received    //    // videos for a better user experience. This mode will kick in only when CPU overuse is reported in
the    //    // WebRTC statistics for the outbound video
streams.    //    enableAdaptiveMode:
false,
//    //    // Codec specific settings for scalability modes and max
bitrates.    //    av1:
{    //      maxBitratesVideo:
{    //          low:
100000,    //          standard:
300000,    //          high:
1000000,    //          fullHd:
2000000,    //          ultraHd:
4000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
true,    //      useSimulcast:
false,    //      useKSVC:
true    //
},    //    h264:
{    //      maxBitratesVideo:
{    //          low:
200000,    //          standard:
500000,    //          high:
1500000,    //          fullHd:
3000000,    //          ultraHd:
6000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
true    //
},    //    vp8:
{    //      maxBitratesVideo:
{    //          low:
200000,    //          standard:
500000,    //          high:
1500000,    //          fullHd:
3000000,    //          ultraHd:
6000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
false    //
},    //    vp9:
{    //      maxBitratesVideo:
{    //          low:
100000,    //          standard:
300000,    //          high:
1200000,    //          fullHd:
2500000,    //          ultraHd:
5000000,    //          ssHigh:
2500000    //
},    //      scalabilityModeEnabled:
true,    //      useSimulcast:
false,    //      useKSVC:
true    //
},
//    //    // The options can be used to override default thresholds of video thumbnail heights corresponding
to    //    // the video quality levels used in the application. At the time of this writing the allowed levels
are:    //    //      'low' - for the low quality level (180p at the time of this
writing)    //    //      'standard' - for the medium quality level
(360p)    //    //      'high' - for the high quality level
(720p)    //    // The keys should be positive numbers which represent the minimal thumbnail height for the quality
level.    //
//    //    // With the default config value below the application will use 'low' quality until the thumbnails
are    //    // at least 360 pixels tall. If the thumbnail height reaches 720 pixels then the application will switch
to    //    // the high
quality.    //    minHeightForQualityLvl:
{    //        360:
'standard',    //        720:
'high',    //
},
//    //    // Provides a way to set the codec preference
```

```
on mobile devices, both on RN and mobile browser based
endpoint    //    mobileCodecPreferenceOrder: [ 'VP8', 'VP9', 'H264', 'AV1'
],    //
},
// Notification
timeouts    // notificationTimeouts:
{    //     short:
2500,    //     medium:
5000,    //     long:
10000,    //     extraLong:
60000,    //
},
// // Options for the recording limit
notification.    // recordingLimit:
{
//    //    // The recording limit in minutes. Note: This number appears in the notification
text    //    // but doesn't enforce the actual recording time limit. This should be configured
in    //    //
jibri!    //    limit:
60,
//    //    // The name of the app with unlimited
recordings.    //    appName: 'Unlimited recordings
APP',
//    //    // The URL of the app with unlimited
recordings.    //    appURL:
'https://unlimited.recordings.app.com/',    //
},
// Disables or enables RTX (RFC 4588) (defaults to
false).    // disableRtx:
false,
// Moves all Jitsi Meet 'beforeunload' logic (cleanup, leaving, disconnecting, etc) to the 'unload'
event.    // disableBeforeUnloadHandlers:
true,
// Disables or enables TCC support in this client (default:
enabled).    // enableTcc:
true,
// Disables or enables REMB support in this client (default:
enabled).    // enableRemb:
true,
// Enables forced reload of the client when the call is migrated as a result
of    // the bridge going
down.    // enableForcedReload:
true,
// Use TURN/UDP servers for the jitsi-videobridge connection (by
default    // we filter out TURN/UDP because it is usually not needed since
the    // bridge itself is reachable via
UDP)    // useTurnUdp:
false
// Enable support for encoded transform in supported browsers. This
allows    // E2EE to work in Safari if the corresponding flag is enabled in the
browser.    //
Experimental.    // enableEncodedTransformSupport:
false,
//
UI
//
// Disables responsive
tiles.    // disableResponsiveTiles:
false,
// DEPRECATED. Please use `securityUi?.hideLobbyButton`
instead.    // Hides lobby
button.    // hideLobbyButton:
false,
// DEPRECATED. Please use `lobby?.autoKnock`
instead.    // If Lobby is enabled starts knocking
automatically.    // autoKnockLobby:
false,
// DEPRECATED. Please use `lobby?.enableChat`
instead.    // Enable lobby
chat.    // enableLobbyChat:
true,
// DEPRECATED! Use `breakoutRooms.hideAddRoomButton`
instead.    // Hides add breakout room
button    // hideAddRoomButton:
false,
// Require users to always specify a display
name.    // requireDisplayName:
true,
```

```
// Enables webhid functionality for
Audio.    // enableWebHIDFeature:
false,
// DEPRECATED! Use 'welcomePage.disabled'
instead.    // Whether to use a welcome page or not. In case it's false a random
room    // will be joined when no room is
specified.    // enableWelcomePage:
true,
// Configs for welcome
page.    // welcomePage:
{    //     // Whether to disable welcome page. In case it's disabled a random
room    //     // will be joined when no room is
specified.    //     disabled:
false,    //     // If set, landing page will redirect to this
URL.    //     customUrl:
''    //
},
// Configs for the lobby
screen.    // lobby:
{    //     // If Lobby is enabled, it starts knocking automatically. Replaces
`autoKnockLobby`.    //     autoKnock:
false,    //     // Enables the lobby chat. Replaces
`enableLobbyChat`.    //     enableChat:
true,    //
},
// Configs for the security related UI
elements.    // securityUi:
{    //     // Hides the lobby button. Replaces
`hideLobbyButton`.    //     hideLobbyButton:
false,    //     // Hides the possibility to set and enter a lobby
password.    //     disableLobbyPassword:
false,    //
},
// Disable app shortcuts that are registered upon joining a
conference    // disableShortcuts:
false,
// Disable initial browser getUserMedia
requests.    // This is useful for scenarios where users might want to start a conference for screensharing
only    // disableInitialGUM:
false,
// Enabling the close page will ignore the welcome page redirection
when    // a call is
hangup.    // enableClosePage:
false,
// Disable hiding of remote thumbnails when in a 1-on-1 conference
call.    // Setting this to null, will also disable showing the remote
videos    // when the toolbar is shown on mouse
movements    // disable1On1Mode: null | false |
true,
// Default local name to be
displayed    // defaultLocalDisplayName:
'me',
// Default remote name to be
displayed    // defaultRemoteDisplayName: 'Fellow
Jitster',
// Hides the display name from the participant
thumbnail    // hideDisplayName:
false,
// Hides the dominant speaker name badge that hovers above the
toolbox    // hideDominantSpeakerBadge:
false,
// Default language for the user interface. Cannot be
overwritten.    // DEPRECATED! Use the `lang` iframe option directly
instead.    // defaultLanguage:
'en',
// Disables profile and the edit of all fields from the profile settings (display name and
email)    // disableProfile:
false,
// Hides the email section under profile
settings.    // hideEmailInSettings:
false,
// When enabled the password used for locking a room is restricted to up to the number of digits
specified    // default: roomPasswordNumberOfDigits:
false,    // roomPasswordNumberOfDigits:
10,
// Message to show the users. Example: 'The service will be down
for    // maintenance at 01:00 AM
GMT,    // noticeMessage:
```

```
',
// Enables calendar integration, depends on
googleApiApplicationClientID    // and
microsoftApiApplicationClientID    // enableCalendarIntegration:
false,
// Whether to notify when the conference is terminated because it was
destroyed.    // notifyOnConferenceDestruction:
true,
// The client id for the google APIs used for the calendar integration, youtube livestreaming,
etc.    // googleApiApplicationClientID:
'<client_id>',
// Configs for prejoin
page.    // prejoinConfig:
{    //     // When 'true', it shows an intermediate page before joining, where the user can configure their
devices.    //     // This replaces `prejoinPageEnabled`. Defaults to
true.    //     enabled:
true,    //     // Hides the participant name editing field in the prejoin
screen.    //     // If requireDisplayName is also set as true, a name should still be provided
through    //     // either the jwt or the userInfo from the iframe api init object in order for this to have an
effect.    //     hideDisplayName:
false,    //     // List of buttons to hide from the extra join options
dropdown.    //     hideExtraJoinButtons: ['no-audio',
'by-phone'],    //     // Configuration for pre-call
test    //     // By setting preCallTestEnabled, you enable the pre-call test in the prejoin
page.    //     // ICE server credentials need to be provided over the
preCallTestICEUrl    //     preCallTestEnabled:
false,    //     preCallTestICEUrl:
''    //
},
// When 'true', the user cannot edit the display
name.    // (Mainly useful when used in conjunction with the JWT so the JWT name becomes read
only.)    // readOnlyName:
false,
// If etherpad integration is enabled, setting this to true
will    // automatically open the etherpad when a participant joins.
This    // does not affect the mobile app since opening an
etherpad    // obscures the conference controls -- it's better to let
users    // choose to open the pad on their own in that
case.    // openSharedDocumentOnJoin:
false,
// If true, shows the unsafe room name warning label when a room name
is    // deemed unsafe (due to the simplicity in the name) and a password is
not    // set or the lobby is not
enabled.    // enableInsecureRoomNameWarning:
false,
// Array with avatar URL prefixes that need to use
CORS.    // corsAvatarURLs: [ 'https://www.gravatar.com/avatar/'
],
// Base URL for a Gravatar-compatible service. Defaults to
Gravatar.    // DEPRECATED! Use `gravatar.baseUrl`
instead.    // gravatarBaseURL:
'https://www.gravatar.com/avatar/',
// Setup for Gravatar-compatible
services.    // gravatar:
{    //     // Defaults to
Gravatar.    //     baseUrl:
'https://www.gravatar.com/avatar/',    //     // True if Gravatar should be
disabled.    //     disabled:
false,    //
},
// App name to be displayed in the invitation email subject, as an alternative
to    //
interfaceConfig.APP_NAME.    // inviteAppName:
null,
// Moved from
interfaceConfig(TOOLBAR_BUTTONS).    // The name of the toolbar buttons to display in the toolbar, including
the    // "More actions" menu. If present, the button will display. Exceptions
are    // "livestreaming" and "recording" which also require being a moderator
and    // some other values in config.js to be enabled. Also, the "profile" button
will    // not display for users with a
JWT.    //
Notes:    // - it's impossible to choose which buttons go in the "More actions"
menu    // - it's impossible to control the placement of
buttons    // - 'desktop' controls the "Share your screen"
button    // - if `toolbarButtons` is undefined, we fallback to enabling all buttons on the
UI    // toolbarButtons:
[    //
'camera',    //
```

```
'chat',    //
'closedcaptions',    //
'desktop',    //
'download',    //
'embedmeeting',    //
'etherpad',    //
'feedback',    //
'filmstrip',    //
'fullscreen',    //
'hangup',    //
'help',    //
'highlight',    //
'invite',    //
'linktosalesforce',    //
'livestreaming',    //
'microphone',    //
'noisesuppression',    //
'participants-pane',    //
'profile',    //
'raisehand',    //
'recording',    //
'security',    //
'select-background',    //
'settings',    //
'shareaudio',    //
'sharedvideo',    //
'shortcuts',    //
'stats',    //
'tileview',    //
'toggle-camera',    //
'videoquality',    //
'whiteboard',    //
],
// Holds values related to toolbar visibility
control.    // toolbarConfig:
{    //     // Moved from
interfaceConfig.INITIAL_TOOLBAR_TIMEOUT    //     // The initial number of milliseconds for the toolbar buttons to be visible on
screen.    //     initialTimeout:
20000,    //     // Moved from
interfaceConfig.TOOLBAR_TIMEOUT    //     // Number of milliseconds for the toolbar buttons to be visible on
screen.    //     timeout:
4000,    //     // Moved from
interfaceConfig.TOOLBAR_ALWAYS_VISIBLE    //     // Whether toolbar should be always visible or should hide after x
milliseconds.    //     alwaysVisible:
false,    //     // Indicates whether the toolbar should still autohide when chat is
open    //     autoHideWhileChatIsOpen:
false,    //
},
// Overrides the buttons displayed in the main toolbar. Depending on the screen size the number of
displayed    // buttons varies from 2 buttons to 8 buttons. Every array in the mainToolbarButtons array will replace
the    // corresponding default buttons configuration matched by the number of buttons specified in the array. Arrays
with    // more than 8 buttons or less then 2 buttons will be ignored. When there there isn't an override for a
certain    // configuration (for example when 3 buttons are displayed) the default jitsi-meet configuration will be
used.    // The order of the buttons in the array is
preserved.    // mainToolbarButtons:
[    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'reactions', 'participants-pane', 'tileview'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'participants-pane', 'tileview'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'raisehand', 'participants-pane'
],    //     [ 'microphone', 'camera', 'desktop', 'chat', 'participants-pane'
],    //     [ 'microphone', 'camera', 'chat', 'participants-pane'
],    //     [ 'microphone', 'camera', 'chat'
],    //     [ 'microphone', 'camera'
]    //
],
// Toolbar buttons which have their click/tap event exposed through the API
on    // `toolbarButtonClicked`. Passing a string for the button key
will    // prevent execution of the click/tap routine; passing an object with `key`
and    // `preventExecution` flag on false will not prevent execution of the
click/tap    // routine. Below array with mixed mode for passing the
buttons.    // buttonsWithNotifyClick:
[    //
'camera',    //
{    //         key:
'chat',    //         preventExecution:
false    //
},    //
{    //         key:
'closedcaptions',    //         preventExecution:
```

```
true    //
},    //
'desktop',    //
'download',    //
'embedmeeting',    //
'end-meeting',    //
'etherpad',    //
'feedback',    //
'filmstrip',    //
'fullscreen',    //
'hangup',    //
'hangup-menu',    //
'help',    //
{    //        key:
'invite',    //        preventExecution:
false    //
},    //
'livestreaming',    //
'microphone',    //
'mute-everyone',    //
'mute-video-everyone',    //
'noisesuppression',    //
'participants-pane',    //
'profile',    //
{    //        key:
'raisehand',    //        preventExecution:
true    //
},    //
'recording',    //
'security',    //
'select-background',    //
'settings',    //
'shareaudio',    //
'sharedvideo',    //
'shortcuts',    //
'stats',    //
'tileview',    //
'toggle-camera',    //
'videoquality',    //    // The add passcode button from the security
dialog.    //
{    //        key:
'add-passcode',    //        preventExecution:
false    //
},    //
'whiteboard',    //
],
// Participant context menu buttons which have their click/tap event exposed through the API
on    // `participantMenuButtonClick`. Passing a string for the button key
will    // prevent execution of the click/tap routine; passing an object with `key`
and    // `preventExecution` flag on false will not prevent execution of the
click/tap    // routine. Below array with mixed mode for passing the
buttons.    // participantMenuButtonsWithNotifyClick:
[    //
'allow-video',    //
{    //        key:
'ask-unmute',    //        preventExecution:
false    //
},    //
'conn-status',    //
'flip-local-video',    //
'grant-moderator',    //
{    //        key:
'kick',    //        preventExecution:
true    //
},    //
{    //        key:
'hide-self-view',    //        preventExecution:
false    //
},    //
'mute',    //
'mute-others',    //
'mute-others-video',    //
'mute-video',    //
'pinToStage',    //
'privateMessage',    //
{    //        key:
'remote-control',    //        preventExecution:
false    //
```

```
},    //
'send-participant-to-room',    //
'verify',    //
],
// List of pre meeting screens buttons to hide. The values must be one or more of the 5 allowed
buttons:    // 'microphone', 'camera', 'select-background', 'invite',
'settings'    // hiddenPremeetingButtons:
[],
// An array with custom option buttons for the participant context
menu    // type:  Array<{ icon: string; id: string; text: string;
}>    // customParticipantMenuButtons:
[],
// An array with custom option buttons for the
toolbar    // type:  Array<{ icon: string; id: string; text: string; backgroundColor?: string;
}>    // customToolbarButtons:
[],
//
Stats
//
// Whether to enable stats collection or not in the
TraceablePeerConnection.    // This can be useful for debugging purposes (post-processing/analysis
of    // the webrtc stats) as it is done in the jitsi-meet-torture
bandwidth    // estimation
tests.    // gatherStats:
false,
// The interval at which PeerConnection.getStats() is called. Defaults to
10000    // pcStatsInterval:
10000,
// Enables sending participants' display names to
stats    // enableDisplayNameInStats:
false,
// Enables sending participants' emails (if available) to stats and other
analytics    // enableEmailInStats:
false,
// faceLandmarks:
{    //     // Enables sharing your face coordinates. Used for centering faces within a
video.    //     enableFaceCentering:
false,
//     // Enables detecting face expressions and sharing data with other
participants    //     enableFaceExpressionsDetection:
false,
//     // Enables displaying face expressions in speaker
stats    //     enableDisplayFaceExpressions:
false,
//     // Enable rtc stats for face
landmarks    //     enableRTCStats:
false,
//     // Minimum required face movement percentage threshold for sending new face centering coordinates
data.    //     faceCenteringThreshold:
10,
//     // Milliseconds for processing a new image capture in order to detect face coordinates if they
exist.    //     captureInterval:
1000,    //
},
// Controls the percentage of automatic feedback shown to
participants.    // The default value is 100%. If set to 0, no automatic feedback will be
requested    // feedbackPercentage:
100,
//
Privacy
//
// If third party requests are disabled, no other server will be
contacted.    // This means avatars will be locally generated and external stats
integration    // will not
function.    // disableThirdPartyRequests:
false,

// Peer-To-Peer mode: used (if enabled) when there are just 2
participants.
//
p2p:
{        // Enables peer to peer mode. When enabled the system will try
to        // establish a direct connection when there are exactly 2
participants        // in the room. If that succeeds the conference will stop sending
data        // through the JVB and use the peer to peer connection instead. When
a        // 3rd participant joins the conference will be moved back to the
JVB        //
connection.        enabled:
```

```
true,
// Sets the ICE transport policy for the p2p connection. At the
time        // of this writing the list of possible values are 'all' and
'relay',        // but that is subject to change in the future. The enum is defined
in        // the WebRTC
standard:        //
https://www.w3.org/TR/webrtc/#rtcicetransportpolicy-enum.        // If not set, the effective value is
'all'.        // iceTransportPolicy:
'all',
// Provides a way to set the codec preference on mobile devices, both on RN and mobile browser
based        //
endpoints.        // mobileCodecPreferenceOrder: [ 'H264', 'VP8', 'VP9', 'AV1'
],
//        // Provides a way to set the codec preference on desktop based
endpoints.        // codecPreferenceOrder: [ 'AV1', 'VP9', 'VP8', 'H264
],
// Provides a way to set the codec for
screenshare.        // screenshareCodec:
'AV1',        // mobileScreenshareCodec:
'VP8',
// How long we're going to wait, before going back to P2P after the
3rd        // participant has left the conference (to filter out page
reload).        // backToP2PDelay:
5,
// The STUN servers that will be used in the peer to peer
connections        stunServers:
[
// { urls: 'stun:jitsi-gtw.inovamesh.cloud:3478'
},            { urls: 'stun:meet-jit-si-turnrelay.jitsi.net:443'
},
],
},
analytics:
{        // True if the analytics should be
disabled        // disabled:
false,
// Matomo
configuration:        // matomoEndpoint:
'https://your-matomo-endpoint/',        // matomoSiteID:
'42',
// The Amplitude APP
Key:        // amplitudeAPPKey:
'<APP_KEY>',
// Enables Amplitude UTM
tracking:        // Default value is
false.        // amplitudeIncludeUTM:
false,
// Obfuscates room name sent to analytics (amplitude,
rtcstats)        // Default value is
false.        // obfuscateRoomName:
false,
// Configuration for the rtcstats
server:        // By enabling rtcstats server every time a conference is joined the
rtcstats        // module connects to the provided rtcstatsEndpoint and sends statistics
regarding        // PeerConnection states along with getStats metrics polled at the
specified        //
interval.        // rtcstatsEnabled:
false,        // rtcstatsStoreLogs:
false,
// In order to enable rtcstats one needs to provide a endpoint
url.        // rtcstatsEndpoint:
wss://rtcstats-server-pilot.jitsi.net/,
// The interval at which rtcstats will poll getStats, defaults to
10000ms.        // If the value is set to 0 getStats won't be polled and the rtcstats
client        // will only send data related to RTCPeerConnection
events.        // rtcstatsPollInterval:
10000,
// This determines if rtcstats sends the SDP to the rtcstats server or
replaces        // all SDPs with an empty string
instead.        // rtcstatsSendSdp:
false,
// Array of script URLs to load as lib-jitsi-meet "analytics
handlers".        // scriptURLs:
[        //
"https://example.com/my-custom-analytics.js",        //
],
// By enabling watchRTCEnabled option you would want to use watchRTC
feature        // This would also require to configure
```

```
watchRTCConfigParams.        // Please remember to keep rtcstatsEnabled disabled for watchRTC to
work.        // watchRTCEnabled:
false,
},
// Logs that should go be passed through the 'log' event if a handler is defined for
it    // apiLogLevels: ['warn', 'log', 'error', 'info',
'debug'],
// Information about the jitsi-meet instance we are connecting to,
including    // the user region as seen by the
server.    // deploymentInfo:
{    //     shard:
"shard1",    //     region:
"europe",    //     userRegion:
"asia",    //
},
// Array<string> of disabled
sounds.    // Possible
values:    // -
'ASKED_TO_UNMUTE_SOUND'    // -
'E2EE_OFF_SOUND'    // -
'E2EE_ON_SOUND'    // -
'INCOMING_MSG_SOUND'    // -
'KNOCKING_PARTICIPANT_SOUND'    // -
'LIVE_STREAMING_OFF_SOUND'    // -
'LIVE_STREAMING_ON_SOUND'    // -
'NO_AUDIO_SIGNAL_SOUND'    // -
'NOISY_AUDIO_INPUT_SOUND'    // -
'OUTGOING_CALL_EXPIRED_SOUND'    // -
'OUTGOING_CALL_REJECTED_SOUND'    // -
'OUTGOING_CALL_RINGING_SOUND'    // -
'OUTGOING_CALL_START_SOUND'    // -
'PARTICIPANT_JOINED_SOUND'    // -
'PARTICIPANT_LEFT_SOUND'    // -
'RAISE_HAND_SOUND'    // -
'REACTION_SOUND'    // -
'RECORDING_OFF_SOUND'    // -
'RECORDING_ON_SOUND'    // -
'TALK_WHILE_MUTED_SOUND'    // disabledSounds:
[],
// DEPRECATED! Use `disabledSounds`
instead.    // Decides whether the start/stop recording audio notifications should play on
record.    // disableRecordAudioNotification:
false,
// DEPRECATED! Use `disabledSounds`
instead.    // Disables the sounds that play when other participants join or leave
the    // conference (if set to true, these sounds will not be
played).    // disableJoinLeaveSounds:
false,
// DEPRECATED! Use `disabledSounds`
instead.    // Disables the sounds that play when a chat message is
received.    // disableIncomingMessageSound:
false,
// Information for the chrome extension
banner    // chromeExtensionBanner:
{    //     // The chrome extension to be installed
address    //     url:
'https://chrome.google.com/webstore/detail/jitsi-meetings/kglhbbefdnlheedjiejgomgmfplipfeb',    //     edgeUrl:
'https://microsoftedge.microsoft.com/addons/detail/jitsi-meetings/eeecajlpbgjppibfledfihobcabccihn',
//     // Extensions info which allows checking if they are installed or
not    //     chromeExtensionsInfo:
[    //
{    //             id:
'kglhbbefdnlheedjiejgomgmfplipfeb',    //             path:
'jitsi-logo-48x48.png',    //
},    //         // Edge extension
info    //
{    //             id:
'eeecajlpbgjppibfledfihobcabccihn',    //             path:
'jitsi-logo-48x48.png',    //
},    //
]    //
},
// e2ee:
{    //   labels:
{    //     description:
'',    //     label:
'',    //     tooltip:
'',    //     warning:
```

```
'',    //
},    //   externallyManagedKey:
false,    //   disabled:
false,    //
},
// Options related to end-to-end (participant to participant)
ping.    // e2eping:
{    //   // Whether ene-to-end pings should be
enabled.    //   enabled:
false,
//    //   // The number of responses to wait
for.    //   numRequests:
5,
//    //   // The max conference size in which e2e pings will be
sent.    //   maxConferenceSize:
200,
//    //   // The maximum number of e2e ping messages per second for the whole conference to aim
for.    //   // This is used to control the pacing of messages in order to reduce the load on the
backend.    //   maxMessagesPerSecond:
250,    //
},
// If set, will attempt to use the provided video input device label
when    // triggering a screenshare, instead of proceeding through the normal
flow    // for obtaining a desktop
stream.    // NOTE: This option is experimental and is currently intended for
internal    // use
only.    // _desktopSharingSourceDevice:
'sample-id-or-label',
// DEPRECATED! Use deeplinking.disabled
instead.    // If true, any checks to handoff to another application will be
prevented    // and instead the app will continue to display in the current
browser.    // disableDeepLinking:
false,
// The deeplinking
config.    // For information about the properties
of    // deeplinking.[ios/android].dynamicLink
check:    //
https://firebase.google.com/docs/dynamic-links/create-manually    // deeplinking:
{
//    //     // The desktop deeplinking config, disabled by
default.    //     desktop:
{    //         appName: 'Jitsi
Meet',    //         appScheme:
'jitsi-meet,    //         download:
{    //
linux:    //
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet-x86_64.AppImage',    //             macos:
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet.dmg',    //             windows:
'https://github.com/jitsi/jitsi-meet-electron/releases/latest/download/jitsi-meet.exe'    //
},    //         enabled:
false    //
},    //     // If true, any checks to handoff to another application will be
prevented    //     // and instead the app will continue to display in the current
browser.    //     disabled:
false,
//     // whether to hide the logo on the deep linking
pages.    //     hideLogo:
false,
//     // The ios deeplinking
config.    //     ios:
{    //         appName: 'Jitsi
Meet',    //         // Specify mobile app scheme for opening the app from the mobile
browser.    //         appScheme:
'org.jitsi.meet',    //         // Custom URL for downloading ios mobile
app.    //         downloadLink:
'https://itunes.apple.com/us/app/jitsi-meet/id1165103905',    //         dynamicLink:
{    //             apn:
'org.jitsi.meet',    //             appCode:
'w2atb',    //             customDomain:
undefined,    //             ibi:
'com.atlassian.JitsiMeet.ios',    //             isi:
'1165103905'    //
}    //
},
//     // The android deeplinking
config.    //     android:
{    //         appName: 'Jitsi
Meet',    //         // Specify mobile app scheme for opening the app from the mobile
```

```
browser.    //         appScheme:
'org.jitsi.meet',    //         // Custom URL for downloading android mobile
app.    //         downloadLink:
'https://play.google.com/store/apps/details?id=org.jitsi.meet',    //         // Android app package
name.    //         appPackage:
'org.jitsi.meet',    //         fDroidUrl:
'https://f-droid.org/en/packages/org.jitsi.meet/',    //         dynamicLink:
{    //             apn:
'org.jitsi.meet',    //             appCode:
'w2atb',    //             customDomain:
undefined,    //             ibi:
'com.atlassian.JitsiMeet.ios',    //             isi:
'1165103905'    //
}    //
}    //
},
// // The terms, privacy and help centre
URL's.    // legalUrls:
{    //     helpCentre:
'https://web-cdn.jitsi.net/faq/meet-faq.html',    //     privacy:
'https://jitsi.org/meet/privacy',    //     terms:
'https://jitsi.org/meet/terms'    //
},
// A property to disable the right click context menu for
localVideo    // the menu has option to flip the locally seen video for local
presentations    // disableLocalVideoFlip:
false,
// A property used to unset the default flip state of the local
video.    // When it is set to 'true', the local(self) video will not be mirrored
anymore.    // doNotFlipLocalVideo:
false,
// Mainly privacy related
settings
// Disables all invite functions from the app (share, invite, dial
out...etc)    // disableInviteFunctions:
true,
// Disables storing the room name to the recents list. When in an iframe this is ignored
and    // the room is never stored in the recents
list.    // doNotStoreRoom:
true,
// Deployment specific
URLs.    // deploymentUrls:
{    //    // If specified a 'Help' button will be displayed in the overflow menu with a link to the specified URL
for    //    // user
documentation.    //    userDocumentationURL:
'https://docs.example.com/video-meetings.html',    //    // If specified a 'Download our apps' button will be displayed in the overflow menu with a
link    //    // to the specified URL for an app download
page.    //    downloadAppsUrl:
'https://docs.example.com/our-apps.html',    //
},
// Options related to the remote participant
menu.    // remoteVideoMenu:
{    //     // Whether the remote video context menu to be rendered or
not.    //     disabled:
true,    //     // If set to true the 'Switch to visitor' button will be
disabled.    //     disableDemote:
true,    //     // If set to true the 'Kick out' button will be
disabled.    //     disableKick:
true,    //     // If set to true the 'Grant moderator' button will be
disabled.    //     disableGrantModerator:
true,    //     // If set to true the 'Send private message' button will be
disabled.    //     disablePrivateChat:
true,    //
},
// Endpoint that enables support for salesforce integration with in-meeting resource
linking    // This is required
for:    // listing the most recent records -
salesforceUrl/records/recents    // searching records -
salesforceUrl/records?text=${text}    // retrieving record details -
salesforceUrl/records/${id}?type=${type}    // and linking the meeting -
salesforceUrl/sessions/${sessionId}/records/${id}
//    // salesforceUrl:
'https://api.example.com/',
// If set to true all muting operations of remote participants will be
disabled.    // disableRemoteMute:
true,

/**     External API url used to receive branding specific
```

```
information.     If there is no url set or there are missing fields, the defaults are
applied.     The config file should be in
JSON.     None of the fields are mandatory and the response must have the
shape:
{        // Whether participant can only send group chat message if `send-groupchat` feature is enabled in
jwt.        groupChatRequiresPermission:
false,        // Whether participant can only create polls if `create-polls` feature is enabled in
jwt.        pollCreationRequiresPermission:
false,        // The domain url to apply (will replace the domain in the sharing conference link/embed
section)        inviteDomain:
'example-company.org',        // The hex value for the colour used as
background        backgroundColor:
'#fff',        // The url for the image used as
background        backgroundImageUrl:
'https://example.com/background-img.png',        // The anchor url used when clicking the logo
image        logoClickUrl:
'https://example-company.org',        // The url used for the image used as
logo        logoImageUrl:
'https://example.com/logo-img.png',        // Overwrite for pool of background images for
avatars        avatarBackgrounds: ['url(https://example.com/avatar-background-1.png)',
'#FFF'],        // The lobby/prejoin screen
background        premeetingBackground:
'url(https://example.com/premeeting-background.png)',        // A list of images that can be used as video
backgrounds.        // When this field is present, the default images will be replaced with those
provided.        virtualBackgrounds:
['https://example.com/img.jpg'],        // Object containing customized icons that should replace the default
ones.
// The keys need to be the exact same icon names used in
here:        //
https://github.com/jitsi/jitsi-meet/blob/master/react/features/base/icons/svg/index.ts        // To avoid having the icons trimmed or displayed in an
unexpected way, please provide
svg        // files containing svg xml icons in the size that the default icons come
in.        customIcons:
{            IconArrowUp:
'https://example.com/arrow-up.svg',            IconDownload:
'https://example.com/download.svg',            IconRemoteControlStart:
'https://example.com/remote-start.svg',
},        // Object containing a theme's properties. It also supports partial overwrites of the main
theme.        // For a list of all possible theme tokens and their current defaults, please
check:        //
https://github.com/jitsi/jitsi-meet/tree/master/resources/custom-theme/custom-theme.json        // For a short explanations on each of the tokens,
please
check:        //
https://github.com/jitsi/jitsi-meet/blob/master/react/features/base/ui/Tokens.ts        // IMPORTANT!: This is work in progress so many of the various
tokens are not yet applied in
code        // or they are partially
applied.        customTheme:
{            palette:
{                ui01: "orange
!important",                ui02:
"maroon",                surface02:
'darkgreen',                ui03:
"violet",                ui04:
"magenta",                ui05:
"blueviolet",                action01:
'green',                action01Hover:
'lightgreen',                disabled01:
'beige',                success02:
'cadetblue',                action02Hover:
'aliceblue',
},            typography:
{                labelRegular:
{                    fontSize:
25,                    lineHeight:
30,                    fontWeight:
500,
}
}
}
}
*/    // dynamicBrandingUrl:
'',
// A list of allowed URL domains for shared
video.
//    //
NOTE:    // '*' is allowed value and it will allow any URL to be used for shared video. We do not recommend using
'*',    // use it at your own
risk!    // sharedVideoAllowedURLDomains: [
```

```
],
// Options related to the participants
pane.    // participantsPane:
{    //     // Enables
feature    //     enabled:
true,    //     // Hides the moderator settings
tab.    //     hideModeratorSettingsTab:
false,    //     // Hides the more actions
button.    //     hideMoreActionsButton:
false,    //     // Hides the mute all
button.    //     hideMuteAllButton:
false,    //
},
// Options related to the breakout rooms
feature.    // breakoutRooms:
{    //     // Hides the add breakout room button. This replaces
`hideAddRoomButton`.    //     hideAddRoomButton:
false,    //     // Hides the auto assign participants
button.    //     hideAutoAssignButton:
false,    //     // Hides the join breakout room
button.    //     hideJoinRoomButton:
false,    //
},
// When true, virtual background feature will be
disabled.    // disableVirtualBackground:
false,
// When true the user cannot add more images to be used as virtual
background.    // Only the default ones from will be
available.    // disableAddingBackgroundImages:
false,
// Sets the background transparency level. '0' is fully transparent, '1' is
opaque.    // backgroundAlpha:
1,
// The URL of the moderated rooms microservice, if available. If
it    // is present, a link to the service will be rendered on the welcome
page,    // otherwise the app doesn't render
it.    // moderatedRoomServiceUrl:
'https://moderated.jitsi-gtw.inovamesh.cloud',
// If true, tile view will not be enabled automatically when the participants count threshold is
reached.    // disableTileView:
true,
// If true, the tiles will be displayed contained within the available space rather than enlarged to cover
it,    // with a 16:9 aspect ratio (old
behaviour).    // disableTileEnlargement:
true,
// Controls the visibility and behavior of the top header conference info
labels.    // If a label's id is not in any of the 2 arrays, it will not be visible at all on the
header.    // conferenceInfo:
{    //     // those labels will not be hidden in tandem with the
toolbox.    //     alwaysVisible: ['recording',
'raised-hands-count'],    //     // those labels will be auto-hidden in tandem with the toolbox
buttons.    //     autoHide:
[    //
'subject',    //
'conference-timer',    //
'participants-count',    //
'e2ee',    //
'video-quality',    //
'insecure-room',    //
'highlight-moment',    //
'top-panel-toggle',    //
]    //
},
// Hides the conference
subject    // hideConferenceSubject:
false,
// Hides the conference
timer.    // hideConferenceTimer:
false,
// Hides the recording
label    // hideRecordingLabel:
false,
// Hides the participants
stats    // hideParticipantsStats:
true,
// Sets the conference
subject    // subject: 'Conference
Subject',
```

```
// Sets the conference local
subject    // localSubject: 'Conference Local
Subject',
// This property is related to the use case when jitsi-meet is used via the IFrame API. When the property is
true    // jitsi-meet will use the local storage of the host page instead of its own. This option is useful if the
browser    // is not persisting the local storage inside the
iframe.    // useHostPageLocalStorage:
true,
// Etherpad ("shared document")
integration.
//    // If set, add a "Open shared document" link to the bottom right menu
that    // will open an etherpad
document.    // etherpad_base:
'https://your-etherpad-installati.on/p/',
// To enable information about dial-in access to meetings you need to
provide    // dialInNumbersUrl and
dialInConfCodeUrl.    // dialInNumbersUrl returns a json array of numbers that can be used for
dial-in.    // {"countryCode":"US","tollFree":false,"formattedNumber":"+1
123-456-7890"}    // dialInConfCodeUrl is the conference mapper converting a meeting id to a PIN used for
dial-in    // or the other way around (more info in
resources/cloud-api.swagger)
// You can use external service for authentication that will redirect back passing a jwt
token    // You can use tokenAuthUrl config to point to a URL of such
service.    // The URL for the service supports few params which will be filled in by the
code.    //
tokenAuthUrl:    //
'https://myservice.com/auth/{room}?code_challenge_method=S256&code_challenge={code_challenge}&state={state}'    // Supported parameters in
tokenAuthUrl:    //      {room} - will be replaced with the room
name    //      {code_challenge} - (A web only). A oauth 2.0 code challenge that will be sent to the service.
See:    //          https://datatracker.ietf.org/doc/html/rfc7636. The code verifier will be saved in the
sessionStorage    //          under key:
'code_verifier'.    //      {state} - A json with the current state before redirecting. Keys that are included in the
state:    //          - room (The current room name as shown in the address
bar)    //          - roomSafe (the backend safe room name to use (lowercase), that is passed to the
backend)    //          - tenant (The tenant if
any)    //          - config.xxx (all config
overrides)    //          - interfaceConfig.xxx (all interfaceConfig
overrides)    //          - ios=true (in case ios mobile app is
used)    //          - android=true (in case android mobile app is
used)    //          - electron=true (when web is loaded in electron
app)    // If there is a logout service you can specify its URL
with:    // tokenLogoutUrl:
'https://myservice.com/logout'    // You can enable tokenAuthUrlAutoRedirect which will detect that you have logged in successfully
before    // and will automatically redirect to the token service to get the token for the
meeting.    // tokenAuthUrlAutoRedirect:
false    // An option to respect the context.tenant jwt field compared to the current tenant from the
url    // tokenRespectTenant:
false,
// You can put an array of values to target different entity types in the invite
dialog.    // Valid values are "phone", "room", "sip", "user", "videosipgw" and
"email"    // peopleSearchQueryTypes: ["user",
"email"],    // Directory endpoint which is called for invite dialog
autocomplete    // peopleSearchUrl:
"https://myservice.com/api/people",    // Endpoint which is called to send invitation
requests    // inviteServiceUrl:
"https://myservice.com/api/invite",
// For external entities (e. g. email), the localStorage key holding the token value for directory
authentication    // peopleSearchTokenLocation:
"mytoken",

// Options related to
visitors.    // visitors:
{    //    // Starts audio/video when the participant is promoted from
visitor.    //    enableMediaOnPromote:
{    //        audio:
true,    //        video:
true    //
},    //
},    // The default type of desktop sharing sources that will be used in the electron
app.    // desktopSharingSources: ['screen',
'window'],
// Disables the echo cancelation for local audio
tracks.    // disableAEC:
true,
// Disables the auto gain control for local audio
tracks.    // disableAGC:
true,
// Disables the audio processing (echo cancelation, auto gain control and noise suppression) for local audio
```

```
tracks.    // disableAP:
true,
// Disables the anoise suppression for local audio
tracks.    // disableNS:
true,
// Replaces the display name with the JID of the
participants.    // displayJids:
true,
// Enables disables talk while muted
detection.    // enableTalkWhileMuted:
true,
// Sets the peer connection ICE transport policy to
"relay".    // forceTurnRelay:
true,
// List of undocumented settings used in
jitsi-meet
/**
_immediateReloadThreshold
deploymentInfo
dialOutAuthUrl
dialOutCodesUrl
dialOutRegionUrl
disableRemoteControl
iAmRecorder
iAmSipGateway
microsoftApiApplicationClientID
*/

/**     * This property can be used to alter the generated meeting invite links (in combination with a branding
domain     * which is retrieved internally by jitsi meet) (e.g.
https://meet.jit.si/someMeeting     * can become
https://brandedDomain/roomAlias)
*/    // brandingRoomAlias:
null,
// List of undocumented settings used in
lib-jitsi-meet
/**
_peerConnStatusOutOfLastNTimeout
_peerConnStatusRtcMuteTimeout
avgRtpStatsN
desktopSharingSources
disableLocalStats
hiddenDomain
hiddenFromRecorderFeatureEnabled
ignoreStartMuted
websocketKeepAlive
websocketKeepAliveUrl
*/

/**     * Default interval (milliseconds) for triggering mouseMoved iframe API
event
*/    mouseMoveCallbackInterval:
1000,

/**        Use this array to configure which notifications will be shown to the
user        The items correspond to the title or description key of that
notification        Some of these notifications also depend on some other internal logic to be displayed or
not,        so adding them here will not ensure they will always be
displayed
A falsy value for this prop will result in having all notifications enabled (e.g null, undefined,
false)
*/    // notifications:
[    //     'connection.CONNFAIL', // shown when the connection
fails,    //     'dialog.cameraConstraintFailedError', // shown when the camera
failed    //     'dialog.cameraNotSendingData', // shown when there's no feed from user's
camera    //     'dialog.kickTitle', // shown when user has been
kicked    //     'dialog.liveStreaming', // livestreaming notifications (pending, on, off,
limits)    //     'dialog.lockTitle', // shown when setting conference password
fails    //     'dialog.maxUsersLimitReached', // shown when maximmum users limit has been
reached    //     'dialog.micNotSendingData', // shown when user's mic is not sending any
audio    //     'dialog.passwordNotSupportedTitle', // shown when setting conference password fails due to password
format    //     'dialog.recording', // recording notifications (pending, on, off,
limits)    //     'dialog.remoteControlTitle', // remote control notifications (allowed, denied, start, stop,
error)    //
'dialog.reservationError',    //     'dialog.screenSharingFailedTitle', // shown when the screen sharing
failed    //     'dialog.serviceUnavailable', // shown when server is not
reachable    //     'dialog.sessTerminated', // shown when there is a failed conference
session    //     'dialog.sessionRestarted', // show when a client reload is initiated because of bridge
```

```
migration    //     'dialog.tokenAuthFailed', // show when an invalid jwt is
used    //     'dialog.tokenAuthFailedWithReasons', // show when an invalid jwt is used with the reason behind the
error    //     'dialog.transcribing', // transcribing notifications (pending,
off)    //     'dialOut.statusMessage', // shown when dial out status is
updated.    //     'liveStreaming.busy', // shown when livestreaming service is
busy    //     'liveStreaming.failedToStart', // shown when livestreaming fails to
start    //     'liveStreaming.unavailableTitle', // shown when livestreaming service is not
reachable    //     'lobby.joinRejectedMessage', // shown when while in a lobby, user's request to join is
rejected    //     'lobby.notificationTitle', // shown when lobby is toggled and when join requests are allowed /
denied    //     'notify.audioUnmuteBlockedTitle', // shown when mic unmute
blocked    //     'notify.chatMessages', // shown when receiving chat messages while the chat window is
closed    //     'notify.connectedOneMember', // show when a participant
joined    //     'notify.connectedThreePlusMembers', // show when more than 2 participants joined
simultaneously    //     'notify.connectedTwoMembers', // show when two participants joined
simultaneously    //     'notify.dataChannelClosed', // shown when the bridge channel has been
disconnected    //     'notify.hostAskedUnmute', // shown to participant when host asks them to
unmute    //     'notify.invitedOneMember', // shown when 1 participant has been
invited    //     'notify.invitedThreePlusMembers', // shown when 3+ participants have been
invited    //     'notify.invitedTwoMembers', // shown when 2 participants have been
invited    //     'notify.kickParticipant', // shown when a participant is
kicked    //     'notify.leftOneMember', // show when a participant
left    //     'notify.leftThreePlusMembers', // show when more than 2 participants left
simultaneously    //     'notify.leftTwoMembers', // show when two participants left
simultaneously    //     'notify.linkToSalesforce', // shown when joining a meeting with salesforce
integration    //     'notify.localRecordingStarted', // shown when the local recording has been
started    //     'notify.localRecordingStopped', // shown when the local recording has been
stopped    //     'notify.moderationInEffectCSTitle', // shown when user attempts to share content during AV
moderation    //     'notify.moderationInEffectTitle', // shown when user attempts to unmute audio during AV
moderation    //     'notify.moderationInEffectVideoTitle', // shown when user attempts to enable video during AV
moderation    //     'notify.moderator', // shown when user gets moderator
privilege    //     'notify.mutedRemotelyTitle', // shown when user is muted by a remote
party    //     'notify.mutedTitle', // shown when user has been muted upon
joining,    //     'notify.newDeviceAudioTitle', // prompts the user to use a newly detected audio
device    //     'notify.newDeviceCameraTitle', // prompts the user to use a newly detected
camera    //     'notify.noiseSuppressionFailedTitle', // shown when failed to start noise
suppression    //     'notify.participantWantsToJoin', // shown when lobby is enabled and participant requests to join
meeting    //     'notify.participantsWantToJoin', // shown when lobby is enabled and participants request to join
meeting    //     'notify.passwordRemovedRemotely', // shown when a password has been removed
remotely    //     'notify.passwordSetRemotely', // shown when a password has been set
remotely    //     'notify.raisedHand', // shown when a participant used raise
hand,    //     'notify.screenShareNoAudio', // shown when the audio could not be shared for the selected
screen    //     'notify.screenSharingAudioOnlyTitle', // shown when the best performance has been affected by screen
sharing    //     'notify.selfViewTitle', // show "You can always un-hide the self-view from
settings"    //     'notify.startSilentTitle', // shown when user joined with no
audio    //     'notify.suboptimalExperienceTitle', // show the browser
warning    //     'notify.unmute', // shown to moderator when user raises hand during AV
moderation    //     'notify.videoMutedRemotelyTitle', // shown when user's video is muted by a remote
party,    //     'notify.videoUnmuteBlockedTitle', // shown when camera unmute and desktop sharing are
blocked    //
'prejoin.errorDialOut',    //
'prejoin.errorDialOutDisconnected',    //
'prejoin.errorDialOutFailed',    //
'prejoin.errorDialOutStatus',    //
'prejoin.errorStatusCode',    //
'prejoin.errorValidation',    //     'recording.busy', // shown when recording service is
busy    //     'recording.failedToStart', // shown when recording fails to
start    //     'recording.unavailableTitle', // shown when recording service is not
reachable    //     'toolbar.noAudioSignalTitle', // shown when a broken mic is
detected    //     'toolbar.noisyAudioInputTitle', // shown when noise is detected for the current
microphone    //     'toolbar.talkWhileMutedPopup', // shown when user tries to speak while
muted    //     'transcribing.failed', // shown when transcribing
fails    //
],
// List of notifications to be disabled. Works in tandem with the above
setting.    // disabledNotifications:
[],
// Prevent the filmstrip from autohiding when screen width is under a certain
threshold    // disableFilmstripAutohiding:
false,
// filmstrip:
{    //     // Disable the vertical/horizontal
filmstrip.    //     disabled:
false,    //     // Disables user resizable filmstrip. Also, allows configuration of the
filmstrip    //     // (width, tiles aspect ratios) through the interfaceConfig
options.    //     disableResizable:
false,
//     // Disables the stage
filmstrip    //     // (displaying multiple participants on stage besides the vertical
```

```
filmstrip)    //     disableStageFilmstrip:
false,
//     // Default number of participants that can be displayed on
stage.    //     // The user can change this in settings. Number must be between 1 and
6.    //     stageFilmstripParticipants:
1,
//     // Disables the top panel (only shown when a user is sharing their
screen).    //     disableTopPanel:
false,
//     // The minimum number of participants that must be in the call
for    //     // the top panel layout to be
used.    //     minParticipantCountForTopPanel:
50,    //
},
// Tile view related config
options.    // tileView:
{    //     // Whether tileview should be
disabled.    //     disabled:
false,    //     // The optimal number of tiles that are going to be shown in tile view. Depending on the screen size it
may    //     // not be possible to show the exact number of participants specified
here.    //     numberOfVisibleTiles:
25,    //
},
// Specifies whether the chat emoticons are disabled or
not    // disableChatSmileys:
false,
// Settings for the GIPHY
integration.    // giphy:
{    //     // Whether the feature is enabled or
not.    //     enabled:
false,    //     // SDK API Key from
Giphy.    //     sdkKey:
'',    //     // Display mode can be one
of:    //     // - tile: show the GIF on the tile of the participant that sent
it.    //     // - chat: show the GIF as a message in
chat    //     // - all: all of the above. This is the default
option    //     displayMode:
'all',    //     // How long the GIF should be displayed on the tile (in
milliseconds).    //     tileTime:
5000,    //     // Limit results by rating: g, pg, pg-13, r. Default value:
g.    //     rating:
'pg',    //
},
//
Logging    // logging:
{    //     // Default log level for the app and
lib-jitsi-meet.    //     defaultLogLevel:
'trace',    //     // Option to disable
LogCollector.    //     //disableLogCollector:
true,    //     // Individual loggers are
customizable.    //     loggers:
{    //         // The following are too verbose in their logging with the default
level.    //         'modules/RTC/TraceablePeerConnection.js':
'info',    //         'modules/xmpp/strophe.util.js':
'log',    //
},    //
},
// Application logo
url    // defaultLogoUrl:
'images/watermark.svg',
// Settings for the Excalidraw whiteboard
integration.    // whiteboard:
{    //     // Whether the feature is enabled or
not.    //     enabled:
true,    //     // The server used to support whiteboard
collaboration.    //     //
https://github.com/jitsi/excalidraw-backend    //     collabServerBaseUrl:
'https://excalidraw-backend.example.com',    //     // The user access limit to the whiteboard, introduced as a
means    //     // to control the
performance.    //     userLimit:
25,    //     // The url for more info about the whiteboard and its usage
limitations.    //     limitUrl:
'https://example.com/blog/whiteboard-limits',    //
},
// The watchRTC initialize config params as described
:    //
https://testrtc.com/docs/installing-the-watchrtc-javascript-sdk/#h-set-up-the-sdk    //
https://www.npmjs.com/package/@testrtc/watchrtc-sdk    // watchRTCConfigParams:
```

```
{    //         /** Watchrtc api key
*/    //         rtcApiKey:
string;    //         /** Identifier for the session
*/    //         rtcRoomId?:
string;    //         /** Identifier for the current peer
*/    //         rtcPeerId?:
string;    //
/**    //          * ["tag1", "tag2",
"tag3"]    //          * @deprecated use 'keys'
instead    //
*/    //         rtcTags?:
string[];    //         /** { "key1": "value1", "key2": "value2"}
*/    //         keys?:
any;    //         /** Enables additional logging
*/    //         debug?:
boolean;    //         rtcToken?:
string;    //
/**    //          * @deprecated No longer needed. Use "proxyUrl"
instead.    //
*/    //         wsUrl?:
string;    //         proxyUrl?:
string;    //         console?:
{    //             level:
string;    //             override:
boolean;    //
};    //         allowBrowserLogCollection?:
boolean;    //         collectionInterval?:
number;    //         logGetStats?:
boolean;    //
},
// Hide login button on auth dialog, you may want to enable this if you are using JWT tokens to authenticate
users    // hideLoginButton:
true,
// If true remove the tint foreground on focused user camera in
filmstrip    // disableCameraTintForeground:
false,};

// Set the default values for JaaS
customersif (enableJaaS)
{    config.dialInNumbersUrl =
'https://conference-mapper.jitsi.net/v1/access/dids';    config.dialInConfCodeUrl =
'https://conference-mapper.jitsi.net/v1/access';    config.roomPasswordNumberOfDigits = 10; // skip re-adding it (do not remove
comment)}
</script><!-- adapt to your needs, i.e. set hosts and bosh path
-->    <script>/* eslint-disable no-unused-vars, no-var, max-len
*//* eslint sort-keys: ["error", "asc", {"caseSensitive": false}]
*/
/**
*
!!!IMPORTANT!!!
* * This file is considered deprecated. All options will eventually be moved
to * config.js, and no new options should be added
here.
*/
var interfaceConfig =
{    APP_NAME: 'Jitsi
Meet',    AUDIO_LEVEL_PRIMARY_COLOR:
'rgba(255,255,255,0.4)',    AUDIO_LEVEL_SECONDARY_COLOR:
'rgba(255,255,255,0.2)',

/**     * A UX mode where the last screen share participant is
automatically     * pinned. Valid values are the string "remote-only" so remote
participants     * get pinned but not local, otherwise any truthy value for all
participants,     * and any falsy value to disable the
feature.
*     * Note: this mode is experimental and subject to
breakage.
*/    AUTO_PIN_LATEST_SCREEN_SHARE:
'remote-only',    BRAND_WATERMARK_LINK:
'',
CLOSE_PAGE_GUEST_HINT: false, // A html text to be shown to guests on the close page, false disables
it
DEFAULT_BACKGROUND:
'#040404',    DEFAULT_WELCOME_PAGE_LOGO_URL:
'images/watermark.svg',
DISABLE_DOMINANT_SPEAKER_INDICATOR:
false,
```

```
/**     * If true, notifications regarding joining/leaving are no longer
displayed.
*/    DISABLE_JOIN_LEAVE_NOTIFICATIONS:
false,

/**     * If true, presence status: busy, calling, connected etc. is not
displayed.
*/    DISABLE_PRESENCE_STATUS:
false,

/**     * Whether the speech to text transcription subtitles panel is
disabled.     * If {@code undefined}, defaults to {@code
false}.
*     * @type
{boolean}
*/    DISABLE_TRANSCRIPTION_SUBTITLES:
false,

/**     * Whether or not the blurred video background for large video should
be     * displayed on browsers that can support
it.
*/    DISABLE_VIDEO_BACKGROUND:
false,
DISPLAY_WELCOME_FOOTER:
true,    DISPLAY_WELCOME_PAGE_ADDITIONAL_CARD:
false,    DISPLAY_WELCOME_PAGE_CONTENT:
false,    DISPLAY_WELCOME_PAGE_TOOLBAR_ADDITIONAL_CONTENT:
false,
ENABLE_DIAL_OUT:
true,
FILM_STRIP_MAX_HEIGHT:
120,
GENERATE_ROOMNAMES_ON_WELCOME_PAGE:
true,

/**     * Hide the invite prompt in the header when alone in the
meeting.
*/    HIDE_INVITE_MORE_HEADER:
false,
JITSI_WATERMARK_LINK:
'https://jitsi.org',
LANG_DETECTION: true, // Allow i18n to detect the system
language    LOCAL_THUMBNAIL_RATIO: 16 / 9, //
16:9

/**     * Maximum coefficient of the ratio of the large video to the visible
area     * after the large video is scaled to fit the
window.
*     * @type
{number}
*/    MAXIMUM_ZOOMING_COEFFICIENT:
1.3,

/**     * Whether the mobile app Jitsi Meet is to be promoted to
participants     * attempting to join a conference in a mobile Web browser.
If     * {@code undefined}, defaults to {@code
true}.
*     * @type
{boolean}
*/    MOBILE_APP_PROMO:
true,
// Names of browsers which should show a warning stating the current
browser    // has a suboptimal experience. Browsers which are not listed as optimal
or    // unsupported are considered suboptimal. Valid values
are:    // chrome, chromium, electron, firefox , safari,
webkit    OPTIMAL_BROWSERS: [ 'chrome', 'chromium', 'firefox', 'electron', 'safari', 'webkit'
],
POLICY_LOGO:
null,    PROVIDER_NAME:
'Jitsi',

/**     * If true, will display recent
list
*     * @type
{boolean}
*/    RECENT_LIST_ENABLED:
true,    REMOTE_THUMBNAIL_RATIO: 1, //
1:1
```

```
SETTINGS_SECTIONS: [ 'devices', 'language', 'moderator', 'profile', 'calendar', 'sounds', 'more'
],

/**     * Specify which sharing features should be displayed. If the value is not
set     * all sharing features will be shown. You can set [] to disable
all.
*/    // SHARING_FEATURES: ['email', 'url', 'dial-in',
'embed'],
SHOW_BRAND_WATERMARK:
false,

/**     * Decides whether the chrome extension banner should be rendered on the landing page and during the
meeting.     * If this is set to false, the banner will not be rendered at all. If set to true, the check for
extension(s)     * being already installed is done before
rendering.
*/    SHOW_CHROME_EXTENSION_BANNER:
false,
SHOW_JITSI_WATERMARK:
true,    SHOW_POWERED_BY:
false,    SHOW_PROMOTIONAL_CLOSE_PAGE:
false,

/*     * If indicated some of the error dialogs may point to the support URL
for     *
help.
*/    SUPPORT_URL:
'https://community.jitsi.org/',
// Browsers, in addition to those which do not fully support WebRTC,
that    // are not supported and should show the unsupported browser
page.    UNSUPPORTED_BROWSERS:
[],

/**     * Whether to show thumbnails in filmstrip as a column instead of as a
row.
*/    VERTICAL_FILMSTRIP:
true,
// Determines how the video would fit the screen. 'both' would fit the
whole    // screen, 'height' would fit the original video height to the height of
the    // screen, 'width' would fit the original video width to the width of
the    // screen respecting ratio, 'nocrop' would make the video as large
as    // possible and preserve aspect ratio without
cropping.    VIDEO_LAYOUT_FIT:
'both',

/**     * If true, hides the video quality label indicating the resolution
status     * of the current large
video.
*     * @type
{boolean}
*/    VIDEO_QUALITY_LABEL_DISABLED:
false,

/**     * How many columns the tile view can expand to. The respected range
is     * between 1 and
5.
*/    // TILE_VIEW_MAX_COLUMNS:
5,
// List of undocumented
settings
/**
INDICATOR_FONT_SIZES
PHONE_NUMBER_REGEX
*/
// -----------------DEPRECATED CONFIGS BELOW THIS
LINE-----------------------------

/**     * Specify URL for downloading ios mobile
app.
*/    // MOBILE_DOWNLOAD_LINK_IOS:
'https://itunes.apple.com/us/app/jitsi-meet/id1165103905',

/**     * Specify custom URL for downloading android mobile
app.
*/    // MOBILE_DOWNLOAD_LINK_ANDROID:
'https://play.google.com/store/apps/details?id=org.jitsi.meet',

/**     * Specify mobile app scheme for opening the app from the mobile
browser.
```

```
*/    // APP_SCHEME:
'org.jitsi.meet',
// NATIVE_APP_NAME: 'Jitsi
Meet',

/**     * Specify Firebase dynamic link properties for the mobile
apps.
*/    // MOBILE_DYNAMIC_LINK:
{    //    APN:
'org.jitsi.meet',    //    APP_CODE:
'w2atb',    //    CUSTOM_DOMAIN:
undefined,    //    IBI:
'com.atlassian.JitsiMeet.ios',    //    ISI:
'1165103905'    //
},

/**     * Hide the logo on the deep linking
pages.
*/    // HIDE_DEEP_LINKING_LOGO:
false,

/**     * Specify the Android app package
name.
*/    // ANDROID_APP_PACKAGE:
'org.jitsi.meet',

/**     * Specify custom URL for downloading f droid
app.
*/    // MOBILE_DOWNLOAD_LINK_F_DROID:
'https://f-droid.org/packages/org.jitsi.meet/',
// Connection indicators
(    //
CONNECTION_INDICATOR_AUTO_HIDE_ENABLED,    //
CONNECTION_INDICATOR_AUTO_HIDE_TIMEOUT,    // CONNECTION_INDICATOR_DISABLED) got moved to
config.js.
// Please use disableModeratorIndicator from
config.js    // DISABLE_FOCUS_INDICATOR:
false,
// Please use defaultLocalDisplayName from
config.js    // DEFAULT_LOCAL_DISPLAY_NAME:
'me',
// Please use defaultLogoUrl from
config.js    // DEFAULT_LOGO_URL:
'images/watermark.svg',
// Please use defaultRemoteDisplayName from
config.js    // DEFAULT_REMOTE_DISPLAY_NAME: 'Fellow
Jitster',
// Moved to config.js as
`toolbarConfig.initialTimeout`.    // INITIAL_TOOLBAR_TIMEOUT:
20000,
// Please use `liveStreaming.helpLink` from
config.js    // Documentation reference for the live streaming
feature.    // LIVE_STREAMING_HELP_LINK:
'https://jitsi.org/live',
// Moved to config.js as
`toolbarConfig.alwaysVisible`.    // TOOLBAR_ALWAYS_VISIBLE:
false,
// This config was moved to config.js as
`toolbarButtons`.    // TOOLBAR_BUTTONS:
[],
// Moved to config.js as
`toolbarConfig.timeout`.    // TOOLBAR_TIMEOUT:
4000,
// Allow all above example options to include a trailing comma
and    // prevent fear when commenting out the last
value.    // eslint-disable-next-line
sort-keys    makeJsonParserHappy: 'even if last key had a trailing
comma'
// No configuration value should follow this
line.};

/* eslint-enable no-unused-vars, no-var, max-len
*/</script>
<script
src="libs/lib-jitsi-meet.min.js?v=8542"></script>    <script
src="libs/app.bundle.min.js?v=8542"></script>    <title>Jitsi
Meet</title><meta property="og:title" content="Jitsi
Meet"/><meta property="og:image"
```

content="images/jitsilogo.png?v=1"/><meta property="og:description" content="Join a WebRTC video conference powered by the Jitsi Videobridge"/><meta description="Join a WebRTC video conference powered by the Jitsi Videobridge"/><meta itemprop="name" content="Jitsi Meet"/><meta itemprop="description" content="Join a WebRTC video conference powered by the Jitsi Videobridge"/><meta itemprop="image" content="images/jitsilogo.png?v=1"/><link rel="icon" href="images/favicon.svg?v=1">
<template id = "welcome-page-additional-content-template"></template>
<template id = "welcome-page-additional-card-template"></template>
<template id="settings-toolbar-additional-content-template"></template>

</head>
<body> <noscript aria-hidden="true"> JavaScript is disabled. </br>For this site to work you have to enable JavaScript.
</noscript>

</body></html>
-CR-

1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	24/05/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE

SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	19/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	13/07/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/02/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						
TLS13-AES-128-GCM-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe8192	8192	yes	202	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low

TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/06/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS

TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	21/03/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	11:67:ed:ca:35:b3:5f:53:5c:67:40:ef:6a:f3:bc:40:23:bd:7c:0d
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
organizationName	inovamesh.cloud
organizationalUnitName	jitsi-gtw
commonName	jitsi-gtw.inovamesh.cloud
emailAddress	webmaster@jitsi-gtw.inovamesh.cloud
(0)SUBJECT NAME	
organizationName	inovamesh.cloud
organizationalUnitName	jitsi-gtw
commonName	jitsi-gtw.inovamesh.cloud
emailAddress	webmaster@jitsi-gtw.inovamesh.cloud
(0)Valid From	Jun 3 21:17:15 2025 GMT
(0)Valid Till	Jun 1 21:17:15 2035 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(4096 bit)
(0)	RSA Public-Key: (4096 bit)
(0)	Modulus:
(0)	00:c5:07:6d:ff:39:f2:2c:38:f2:57:44:1f:0b:2d:
(0)	8d:d6:8e:27:29:3c:b8:dc:3f:02:fc:01:3f:f2:ef:
(0)	a5:5c:ef:3c:a6:42:9b:8c:f3:fe:48:c9:17:f6:a0:
(0)	11:68:2b:37:c0:9c:f7:05:e9:5b:fb:4a:c6:7d:15:
(0)	e0:00:55:56:e4:bc:29:ff:7d:aa:6b:7c:d2:ce:f7:
(0)	75:59:28:fc:7e:95:93:26:b5:7e:45:2e:42:de:cf:

(0)	3e:88:0f:77:3b:4f:4d:53:4a:d2:a7:e9:01:36:d5:
(0)	c1:ac:1e:b4:cf:1e:f4:b8:e4:57:f5:f1:ab:be:c8:
(0)	7d:16:f1:a9:08:98:72:c9:f7:f7:af:2b:cf:c1:96:
(0)	60:3c:20:2f:4d:9e:95:b1:82:09:91:70:c7:d4:59:
(0)	c4:ae:ee:02:c0:7f:42:3e:f3:43:25:5f:16:26:04:
(0)	4e:68:83:5f:5b:98:a6:4a:b6:e2:3f:a3:31:21:4f:
(0)	53:72:83:46:e0:de:e7:52:0d:4c:34:05:21:32:27:
(0)	32:f5:03:d6:af:19:f4:f9:5c:1c:74:79:a6:23:b2:
(0)	8b:44:f5:dd:cb:cd:4c:ad:2e:c0:d2:b9:88:76:b1:
(0)	72:dc:ad:2c:4a:84:87:83:6d:4e:58:13:74:ae:2b:
(0)	7b:37:32:b3:7f:33:95:c9:93:9b:14:a4:6e:29:03:
(0)	03:4b:53:2c:92:36:3f:d7:90:4c:e2:41:45:06:23:
(0)	a0:59:82:07:45:05:3b:07:9f:d6:db:38:44:75:ef:
(0)	af:fc:39:5e:af:f3:65:3f:2f:c9:16:27:4f:03:45:
(0)	c9:bf:f8:e0:5c:71:1c:ad:5d:7b:fa:ef:82:bb:ba:
(0)	e0:d7:3c:56:66:a3:91:43:d6:32:a3:7f:24:4c:91:
(0)	e2:9e:08:6a:b7:ab:b9:b8:be:66:16:34:c3:ff:85:
(0)	83:b6:fb:1c:1d:cd:d4:7d:ba:a4:2e:3e:ae:62:57:
(0)	ab:d5:64:bb:61:0c:7c:bb:64:5f:d3:17:23:37:0c:
(0)	c3:b5:e0:ca:ea:b1:2d:4a:56:68:17:bd:c3:ca:da:
(0)	39:6d:d6:df:04:80:a3:34:10:da:66:0b:af:ae:14:
(0)	4d:9e:e9:15:65:47:1f:2e:d0:e9:c1:cc:cd:dd:fe:
(0)	b8:9b:f8:73:ad:ce:42:e8:c1:cb:1f:3e:ac:a6:e5:
(0)	98:b3:d6:60:bf:c9:57:c4:24:41:f9:fb:8c:a2:0b:
(0)	19:fa:4a:96:09:43:ed:ba:c4:9f:da:23:af:97:7d:
(0)	a6:24:6f:63:6d:7e:4e:29:cd:90:af:43:50:a2:c2:
(0)	d8:55:b1:d6:7e:9b:c5:f6:53:a7:74:c1:a9:20:7d:
(0)	f9:b9:19:3e:30:86:78:c0:dd:df:27:9d:b7:89:6e:
(0)	b3:02:1f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Subject Alternative Name	DNS:localhost, DNS:jitsi-gtw.inovamesh.cloud
(0)X509v3 Subject Key Identifier	17:3D:1A:71:08:48:10:D3:18:9A:0D:8D:C5:D5:AB:EE:20:02:83:FB
(0)Signature	(512 octets)
(0)	67:cb:9c:69:6a:9c:84:81:92:34:3f:e2:91:87:43:dd
(0)	cd:68:ed:b1:c5:e1:b8:fa:6a:96:09:51:75:6b:93:0b
(0)	05:de:1e:49:26:3b:92:6f:a8:6d:f8:3d:ff:f8:32:07
(0)	f2:a2:ae:53:14:61:95:cc:bf:eb:d2:44:6a:28:aa:70
(0)	f4:2e:1f:da:b4:63:eb:05:d5:73:0b:07:43:26:b0:b0
(0)	57:42:69:f8:30:40:03:a6:d3:6e:a3:50:94:24:3f:80
(0)	da:78:fa:b8:10:30:bd:3d:4a:9c:45:d2:13:a2:03:d0
(0)	6d:97:bd:3d:f8:48:d2:31:74:1a:6d:07:80:18:61:d3
(0)	27:59:2a:a9:e9:82:a9:1f:38:eb:0d:b4:a2:28:7d:87
(0)	8f:75:ef:1d:c2:3a:cc:36:84:d4:02:9a:4f:3a:78:32
(0)	b8:0d:a4:c8:bd:69:02:f3:08:66:0e:7c:f0:9b:8a:7a
(0)	da:39:07:ba:6b:14:bc:44:de:3a:96:03:90:e4:f6:c0
(0)	65:c6:ca:90:31:af:66:70:3f:84:35:ee:66:8b:f5:3f
(0)	a5:5d:e2:9f:2b:32:97:42:7d:64:6b:87:97:59:4b:e2
(0)	15:f9:a1:8b:87:b2:8c:6a:fe:ce:ca:68:f6:b5:2d:a8
(0)	da:6b:b3:5b:ac:88:60:7e:c3:58:1e:3b:ae:e4:e2:d3
(0)	c4:32:aa:94:1c:26:e7:2e:5d:7e:80:fc:f9:28:62:9e
(0)	3a:3a:7a:29:fd:0f:95:50:ec:e2:f5:bd:e4:cc:ef:36
(0)	0d:4a:9a:45:c3:ee:ab:a9:45:5c:31:cd:3b:66:2b:23
(0)	ad:34:16:dd:4c:18:3d:14:43:72:98:5a:28:3c:24:3a
(0)	ba:58:61:4a:62:4a:10:cc:97:88:21:9b:42:5a:48:57

(0)	81:f2:b1:54:e4:d0:37:ef:f5:c1:d3:82:d0:56:49:5b
(0)	9a:5c:16:5e:0f:1f:cb:24:15:11:66:fb:f0:30:e5:9a
(0)	3f:f6:a5:bc:5e:fe:f5:60:df:2a:ec:04:5a:fd:c9:d5
(0)	41:ad:e2:64:b5:88:e3:67:fb:60:16:77:82:ff:18:56
(0)	14:49:68:1d:16:fe:a4:15:15:99:a1:94:89:8a:f6:97
(0)	55:b7:d9:99:29:a7:96:63:53:52:3e:2b:26:cc:65:d1
(0)	ce:37:37:97:04:50:12:4d:f5:1a:7d:01:7d:6c:65:4d
(0)	3f:1a:d0:aa:ab:b8:43:28:a0:61:7f:c2:16:26:be:89
(0)	b0:0b:11:9f:ae:1b:5b:88:60:fe:76:5b:53:1a:af:6e
(0)	2d:50:7b:27:c1:bb:50:e5:00:0c:a2:bc:aa:ed:ab:16
(0)	8e:eb:d9:cb:20:8d:2e:c1:03:24:c0:7b:54:e3:ca:dd

Appendix

Hosts Scanned (DNS)

jitsi-gtw.inovamesh.cloud

Options Profile

I-Mesh Option Profile (Oscar)

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan and Additional TCP Ports: 80, 443, 4443, 5222, 5347, 5349
Scanned UDP Ports:	Standard Scan and Additional UDP Ports: 3478, 4380, 4381, 10000
Scan Dead Hosts:	On
Close Vulnerabilities on Dead Hosts Count:	2
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Include OVAL Checks:	yes
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Standard
Custom:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco/Network SSH:	Enabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Enabled
MySQL:	Enabled
Tomcat Server:	Enabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled
NGINX:	Disabled

Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Cassandra:	Disabled
MarkLogic:	Disabled
DataStax:	Disabled
Prism Central:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	On
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Severity	Level	Description
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.