CERT-EU Security Advisory 2017-016

CISCO WebEx Browser Extension Remote Code Execution Vulnerability

July 20, 2017 — v1.0

History:

- *20/07/2017 — v1.0 – Initial publication*

Summary

A vulnerability in CISCO WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on a targeted system. This vulnerability affects the browser extensions for CISCO WebEx Meetings Server and CISCO WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) and Cisco WebEx Meetings when they are running on Microsoft Windows.

The vulnerability is due to a design defect in the extension. An attacker that can convince a user who has installed these extensions to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser [1]. These vulnerabilities were found by Tavis Ormandy from Google Project Zero and Cris Neckar of Divergent Security.

Products Affected

This vulnerability affects CISCO WebEx extensions for Windows when running on most supported browsers. The affected browsers are Google Chrome and Mozilla Firefox.

The following versions of the CISCO WebEx browser extensions are affected by the vulnerability described in this document:

- versions prior to `1.0.12` of the CISCO WebEx Extension on Google Chrome
- versions prior to `1.0.12` of the CISCO WebEx Extension on Mozilla Firefox

Recommendations

Users who have the WebEx extension for their browsers (Mozilla Firefox, Google Chrome) installed should update immediately to the updated, fixed versions.

Users can use the following steps to determine which versions of the Cisco WebEx extensions are being used:

Chrome users can determine the version of the Cisco WebEx extension for Google Chrome by doing the following:

In Chrome, click the menu button (three dots at the upper right of the application) and choose More Tools > Extensions The extension version is listed next to the Cisco WebEx extension name. The Cisco WebEx extension for Google Chrome identification string, which organizations can use to identify hosts that contain the extension, is the following:

```
jlhmfgmfgeifomenelglieieghnjghma
```

Firefox users can determine the version of the Cisco WebEx extension for Mozilla Firefox by doing the following:

In Firefox, click the menu button (three horizontal bars at the upper right of the application) and choose Add-ons Click the Extensions tab Locate Cisco WebEx Extension in the list of extensions and click the More link to obtain the version information.

There are no workarounds that address this vulnerability. However, Windows users may use Internet Explorer and administrators and users of Windows 10 systems may use Microsoft Edge to join and participate in WebEx sessions because Microsoft Internet Explorer and Microsoft Edge are not affected by this vulnerability. Additionally, administrators and users can remove all WebEx software from a Windows system by using the Meeting Services Removal Tool, which is available from [2].

Non affected versions

Cisco has confirmed that this vulnerability does not affect the following products:

- Cisco WebEx Productivity Tools
- Cisco WebEx browser extensions for Mac or Linux
- Cisco WebEx on Microsoft Edge or Internet Explorer

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170717-webex

[2] https://help.webex.com/docs/DOC-2672