CERT-EU Security Advisory 2017-001

CISCO WebEx Browser Extension Remote Code Execution Vulnerability

February 1, 2017 — v1.1

History:

- *24/01/2017 — v1.0 – Initial publication*
- *31/01/2017 — v1.1 – Updated with information about additional browsers affected*

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 an affected 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) when they are running on Microsoft Windows.

The vulnerability is due to a design defect in an application programing interface (API) response parser within the plugin. An attacker that can convince an affected user 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].

Products Affected

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

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

- versions prior to `1.0.7` of the CISCO WebEx Extension on Google Chrome
- versions prior to `106` of the ActiveTouch General Plugin Container on Mozilla Firefox
- versions prior to `10031.6.2017.0126` of the GpcContainer Class ActiveX control file on Internet Explorer

Recommendations

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

- version `106` of the ActiveTouch General Plugin Container (`10031.6.2017.127`) for Mozilla Firefox
- version `10031.6.2017.0126` of the GpcContainer Class for Microsoft Internet Explorer
- version `1.0.7` of CISCO WebEx Extension for Google Chrome

Administrators and users of Windows 10 systems may utilize Microsoft Edge to join and participate in WebEx sessions as Microsoft Edge is 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].

Customers who currently have web proxies or web gateways in their environment can create a URL filtering policy to block web requests based on the following conditions:

- URL requests **containing** the string pattern:

```
cwcsf-nativemsg-iframe-43c85c0d-d633-af5e-c056-32dc7efc570b.html
```

- URL hostname **not matching** the known customer's WebEx site URL — e.g. `company.webex.com` in:

```
https://company.webex.com/cwcsf-nativemsg-iframe-43c85c0d-d633-af5e-c056-32dc7efc570b.html
```

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex

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