CERT-EU Security Advisory 2018-025

Cisco Webex Player Remote Code Execution Vulnerabilities

September 20, 2018 — v1.0

History:

- *20/09/2018 — v1.0 – Initial publication*

Summary

On 19th of September 2018, Cisco published a security advisory concerning Remote Code Execution Vulnerabilities. These vulnerabilities allow an unauthenticated remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of Webex recording files. An attacker could exploit these vulnerabilities by sending a user an e-mail with a link or attachment containing a malicious file and persuading the user to open the file in the Cisco Webex Player. A successful exploit could allow the attacker to execute arbitrary code on an affected system. Cisco has released software updates that address these vulnerabilities [1].

Technical Details

Cisco WebEx Network Recording Player is a tool to watch, share, and edit Cisco WebEx recordings. The vulnerabilities found to affect the Cisco Webex Network Recording Player for Advanced Recording Format (ARF) are due to improper validation of Webex recording files. The vulnerabilities received the following CVEs: **CVE-2018-15414, CVE-2018-15422 and CVE-2018-15421**. Those can be exploited by threat actors via hyperlinks and e-mail attachments leading to or containing a maliciously crafted file which would give the attackers control of the system once played using the Cisco Webex Player [2].

Products Affected

These vulnerabilities affect ARF recording players available from Cisco Webex Meetings Suite sites, Cisco Webex Meetings Online sites, and Cisco Webex Meetings Server. The following versions of ARF recording players are affected:

- Cisco Webex Meetings Suite (WBS32) - Webex Network Recording Player versions prior to WBS32.15.10
- Cisco Webex Meetings Suite (WBS33) - Webex Network Recording Player versions prior to WBS33.3

- Cisco Webex Meetings Online - Webex Network Recording Player versions prior to 1.3.37
- Cisco Webex Meetings Server - Webex Network Recording Player versions prior to 3.0MR2

To determine which version of the Cisco Webex Network Recording Player (for `.arf` files) is installed, users can open the player and select the Help > About menu.

Recommendations

Cisco has released software updates that address the vulnerabilities described in this advisory. Details about the releases, based on the customer configuration, can be found on the Cisco advisory [1].

More generally, for Cisco products, customers are advised to regularly consult the Cisco security advisories, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution [5].

Workarounds

If for any reason it was not possible to apply the proper patch made available by Cisco, the only possible mitigating action to consider is removing the affected Cisco Webex Network Recording Player and Cisco Webex Player by following the uninstall procedure for the operating system. For example, in Windows, use *Add or Remove Programs* to uninstall the affected players.

To remove Webex software completely from a system, use the Meeting Services Removal Tool (for Microsoft Windows users) or Mac Webex Meeting Application Uninstaller (for Apple Mac OS X users), available for download from the Cisco Collaboration Help article Cisco WebEx and 3rd Party Support Utilities [3].

Removal of the Webex software from a Linux or UNIX-based system can be accomplished by following the steps in the Cisco Collaboration Help article *How Do I Uninstall WebEx Software on a Linux or Unix Based System* [4].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180919-webex

[2] https://news.softpedia.com/news/cisco-patches-network-recording-player-remote-code-execution-vulnerabilities-522787.shtml

[3] https://collaborationhelp.cisco.com/article/en-us/WBX000026396

[4] https://collaborationhelp.cisco.com/article/en-us/WBX28548

[5] https://tools.cisco.com/security/center/publicationListing.x