CERT-EU Security Advisory 2018-013

Cisco WebEx ARF Remote Code Execution Vulnerabilities

May 03, 2018 — v1.0

History:

- *03/05/2018 — v1.0: Initial publication*

Summary

The Cisco WebEx Players are applications that are used to play back WebEx meeting recordings that have been recorded by an online meeting attendee. The records are using the Advanced Recording Format (ARF). On May 2nd, 2018, Cisco published two advisories for remote code execution vulnerabilities:

- CVE-2018-0287 (medium) [1]
- CVE-2018-0264 (critical) [2]

An attacker could exploit these vulnerabilities by sending a link or an e-mail attachment with a malicious ARF file and persuading the target to open the malicious file. Successful exploitation could allow the attacker to execute arbitrary code on the target system.

Products Affected

The following products are affected by both vulnerabilities:

- Cisco WebEx Business Suite meeting sites,
- Cisco WebEx Meetings sites,
- Cisco WebEx Meetings Server,
- Cisco WebEx ARF players.

Regarding the critical vulnerability (CVE-2018-0264), Cisco provides a list of affected client builds:

- Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.4,
- Cisco WebEx Business Suite (WBS32) client builds prior to T32.12,
- Cisco WebEx Meetings with client builds prior to T32.12,
- Cisco WebEx Meeting Server builds prior to 3.0 Patch 1.

Recommendations

Upgrade to the most recent version of Cisco WebEx players:

- Cisco WebEx Business Suite (WBS31) client builds T31.23.4 and later,
- Cisco WebEx Business Suite (WBS32) client builds T32.12 and later,
- Cisco WebEx Meetings with client builds T32.12 and later,
- Cisco WebEx Meeting Server builds 3.0 Patch 1 and later.

Workarounds

There are no known workarounds available. However, users can remove completely all WebEx software by using tools and procedures provided by CISCO:

- On Windows systems, via the Meeting Services Removal Tool [3].
- On Mac systems, via the Mac WebEx Meeting Application Uninstaller [3].
- On UNIX/Linux systems, by following the steps in the Cisco Collaboration Help [4].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-webex-rce

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-war

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

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