Security Advisory 2020-012

Cisco Webex Players Vulnerabilities

March 06, 2020 — v1.0

TLP:WHITE

History:

- *06/03/2020 — v1.0 – Initial publication*

Summary

High serverity vulnerabilities were patched in Cisco Webex video conferencing platform. In particular they affect Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows. If exploited, these could allow an attacker to execute code on the affected systems [1]. The vulnerabilities are tracked as CVE-2020-3127 and CVE-2020-3128 and are both 7.8 out of 10.0 on the CVSS scale [2, 3].

Technical Details

The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.

Products Affected

These vulnerabilities affect the following releases of Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows, which are available from Cisco Webex Meetings sites, Cisco Webex Meetings Online sites, and Cisco Webex Meetings Server [1]:

- Cisco Webex Meetings — all Webex Network Recording Player and Webex Player releases earlier than WBS 39.5.17 or WBS 39.11.0
- Cisco Webex Meetings Online — all Webex Network Recording Player and Webex Player releases earlier than 1.3.49
- Cisco Webex Meetings Server — all Webex Network Recording Player releases earlier than 3.0MR3SecurityPatch1 and 4.0MR2SecurityPatch2

To determine which release of Cisco Webex Network Recording Player or Cisco Webex Player is installed on a system, open the player and choose *Help -> About*.

Recommendations

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities. Users of above mentioned software are advised to upgrade to an appropriate fixed software release as indicated in the Cisco Advisory [1].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200304-webex-player

[2] https://nvd.nist.gov/vuln/detail/CVE-2020-3127

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-3128