CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-047

Cisco Webex Teams Client Vulnerability

October 9, 2020 — v1.0

TLP:WHITE

History:

- *9/10/2020 — v1.0 – Initial publication*

Summary

On 7th of October 2020, Cisco released three security advisories with an impact evaluated as *High* [1]. One of them is impacting Windows client version of *Cisco Webex Teams* [2]. The vulnerability is a DLL Hijacking Vulnerability and could potentially be used by an attacker with a foothold on a system to have another user execute a malicious DLL when *Cisco Webex Teams* starts.

There is no known attacks leveraging this vulnerability or proof-of-concept available for now.

Technical Details

The vulnerability was assigned *CVE-2020-3535* with a CVSS score of 7.8 [3].

There is no technical details available outside of the initial advisory from Cisco. Based on the description, the vulnerability is due to incorrect handling of directory paths at run time – meaning that an attacker can place a malicious file in a folder with write access for everyone and have the application execute it when starting.

If a high-privileged user of the system starts the application, the attacker can escalate his/her privileges on the system.

Products Affected

This vulnerability affects the following Cisco Webex Teams Client for Windows versions:

- 3.0.13464.0 through 3.0.16040.0

Non-Windows versions are not affected.

Recommendations

CERT-EU recommends updating Cisco Webex Teams Client for Windows to the latest version as soon as possible.

References

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

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-dll-drsnH5AN

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3535