CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-016

Critical Vulnerabilities in Cisco Products

March 25, 2021 — v1.0

TLP:WHITE

Summary

On 24th of March 2021, Cisco released several security updates to address several security vulnerabilities [1]. The list includes a critical one, affecting Cisco Jabber Desktop and Mobile Client Software: CVE-2021-1411 with a CVSS score of 9.9 out of 10 [2].

Vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for MacOS, and Cisco Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system with elevated privileges, access sensitive information, intercept protected network traffic, or cause a denial of service (DoS) condition [2].

Technical Details

Critical Vulnerability

CVE-2021-1411 *(CVSS 9.9)*: Cisco Jabber Arbitrary Program Execution Vulnerability

The vulnerability can be only exploited by attackers that are authenticated to an XMPP server used by the vulnerable software which is used to send specially-crafted XMPP messages to a vulnerable device. The flaw could be exploited without user interaction by an authenticated, remote attacker to execute arbitrary code on Windows, macOS, Android, or iOS devices running unpatched Jabber client software.

Other Related Vulnerabilities

CVE-2021-1469 *(CVSS 7.2)*: Arbitrary Program Execution Vulnerability

CVE-2021-1417 *(CVSS 6.5)*: Information Disclosure Vulnerability

CVE-2021-1471 *(CVSS 5.6)*: Certificate Validation Vulnerability

CVE-2021-1418 *(CVSS 4.3)*: Denial of Service Vulnerability

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of these vulnerabilities.

Products Affected

These vulnerabilities affect Cisco Jabber for Windows, Cisco Jabber for MacOS, and Cisco Jabber for mobile platforms [2].

Cisco Jabber Platform	Associated CVE IDs
Windows	CVE-2021-1411, CVE-2021-1417, CVE-2021-1418, CVE-2021-1469, and CVE-2021-1471
MacOS	CVE-2021-1418 and CVE-2021-1471
Android and iOS	CVE-2021-1418 and CVE-2021-1471

Recommendations

Cisco has released software updates that address these critical vulnerabilities [1, 2].

There are no workarounds that address these vulnerabilities.

CERT-EU recommends updating the vulnerable application 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-cisco-jabber-PWrTATTC