Security Advisory 2020-059

Cisco Jabber Desktop and Mobile Client Software Vulnerabilities

December 11, 2020 — v1.0

TLP:WHITE

Summary

On 10th of December, Cisco released an advisory about multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms. These vulnerabilities could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information.

Technical Details

The vulnerabilities are as follows:

- Cisco Jabber Message Handling Arbitrary Program Execution Vulnerability - **CVE-2020-26085** - CVSS Base Score: 9.9 [1]
- Cisco Jabber Message Handling Script Injection Vulnerability - **CVE-2020-27134** - CVSS Base Score: 8.0 [1]
- Cisco Jabber for Windows Custom Protocol Handler Command Injection Vulnerability - **CVE-2020-27133** - CVSS Base Score: 8.8 [1]
- Cisco Jabber Information Disclosure Vulnerability - **CVE-2020-27132** - CVSS Base Score: 6.5 [1]
- Cisco Jabber for Windows Custom Protocol Handler Unauthorized Access Vulnerability - **CVE-2020-27127** - CVSS Base Score: 4.3 [1]

To exploit the first two message handling vulnerabilities, an attacker must be able to send Extensible Messaging and Presence Protocol (XMPP) messages to end-user systems running Cisco Jabber. Attackers may require access to the same XMPP domain or another method of access to be able to send messages to clients. As a result of exploitation, an attacker could cause the application to run an arbitrary executable that already exists within the local file path of the application. The executable would run on the end-user system with the privileges of the user who initiated the Cisco Jabber client application.

Depending on the vulnerability, a successful exploit could allow an attacker from causing the application to execute arbitrary programs on the targeted system, possibly resulting in arbitrary code execution, to causing the application to return sensitive authentication information to another system, possibly for use in further attacks.

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected

by one of the vulnerabilities may not be affected by the other vulnerabilities.

Products Affected

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

Recommendations

Cisco has released free software updates that address the vulnerabilities described in this advisory.

CERT-EU recommends updating Cisco Jabber Desktop and Mobile Client Software to the latest version as soon as possible..

Workarounds

There are no workarounds that address these vulnerabilities.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO#fs