Security Advisory 2020-043

Critical Vulnerabilities in Cisco Products

September 3, 2020 — v1.0

TLP:WHITE

History:

- *03/09/2020 — v1.0 – Initial publication*

Summary

On 29th of August and on 2nd of September, Cisco released several security advisories, updates, and workarounds to address security vulnerabilities including five high severity vulnerabilities, and one critical [1-6]:

- CVE-2020-3495 - Arbitrary Code Execution - CVSS score 9.9 (critical)
- CVE-2020-3566 - Memory Exhaustion - CVSS score 8.6 (high)
- CVE-2020-3530 - Authenticated User Privilege Escalation - CVSS score 8.4 (high)
- CVE-2020-3430 - Command Injection - CVSS score 8.8 (high)
- CVE-2020-3478 - File Overwrite Vulnerability - CVSS score 8.1 (high)
- CVE-2020-3473 - Authenticated User Privilege Escalation - CVSS score 7.8 (high)

Technical Details

CVE-2020-3495 (CVSS Score: Base 9.9)

The vulnerability in Cisco Jabber for Windows is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted Extensible Messaging and Presence Protocol (XMPP) messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution [1].

CVE-2020-3566 (CVSS Score: Base 8.6)

These vulnerabilities in Cisco IOS XR Software are due to the incorrect handling of IGMP packets. An attacker could exploit these vulnerabilities by sending crafted IGMP traffic to an affected device. A successful exploit could allow the attacker to immediately crash the IGMP process or cause memory exhaustion, resulting in other processes becoming unstable. These processes may include (but are not limited to) interior and exterior routing protocols [2].

CVE-2020-3530 (CVSS Score: Base 8.4)

The vulnerability in Cisco IOS XR Software is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorised to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges [3].

CVE-2020-3430 (CVSS Score: Base 8.8)

The vulnerability in Cisco Jabber for Windows is due to improper handling of input to the application protocol handlers. An attacker could exploit this vulnerability by convincing a user to click a link within a message sent by email or other messaging platform. A successful exploit could allow the attacker to execute arbitrary commands on a targeted system with the privileges of the user account that is running the Cisco Jabber client software [4].

CVE-2020-3478 (CVSS Score: Base 8.1)

The vulnerability in the REST API of Cisco Enterprise NFV Infrastructure Software (NFVIS) is due to insufficient authorisation enforcement on an affected system. An attacker could exploit this vulnerability by uploading a file using the REST API. A successful exploit could allow an attacker to overwrite and upload files, which could degrade the functionality of the affected system [5].

CVE-2020-3473 (CVSS Score: Base 7.8)

The vulnerability in Cisco IOS XR Software is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorisation checks [6].

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of these vulnerabilities [1-6].

Products Affected

These vulnerabilities affect several products:

- Cisco Jabber for Windows [1,4];
- Cisco IOS XR Software (if an active interface is configured under multicast routing and it is receiving DVMRP traffic) [2];
- ASR 9000 Series Aggregation Services Routers (32-bit and 64-bit models) [3];
- IOS XR, SW only [3,6];
- Network Convergence System 1000 Series [3];
- Network Convergence System 5000 Series [3];
- Network Convergence System 5500 Series [3, 6];
- Cisco Enterprise NFVIS releases 3.5.1 through 4.1.2. [5];
- 8000 Series Routers [6];
- IOS XRv 9000 Router [6];
- Network Convergence System 540 Routers [6];
- Network Convergence System 560 Routers [6];
- Network Convergence System 4000 Series [6];
- Network Convergence System 6000 Series Routers [6];

Recommendations

Cisco has released free software updates and workarounds that address `CVE-2020-3495`, `CVE-2020-3430`, `CVE-2020-3530`, `CVE-2020-3478` and `CVE-2020-3473` vulnerabilities [1,3-6].

Cisco will release free software updates that address `CVE-2020-3566` vulnerability. Mitigations are available on Cisco advisory as well as indicators of compromise to observe possible exploits of the vulnerability [2].

CERT-EU recommends updating the vulnerable applications and systems or applying workarounds as soon as possible.

References

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

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-cli-privescl-sDVEmhqv%22

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-vY8M4KGB

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-file-overwrite-UONzPMkr

[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-LJtNFjeN