National Cyber Security Centre

2009030200-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Flash Alert

Critical Vulnerabilities in Cisco Products
2020-09-03

Status: TLP-WHITE

NCSC

Threat Type	Cisco have recently released details of a number of security vulnerabilities, including five high severity vulnerabilities, and one critical. • 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)
Products Affected	These vulnerabilities affect the following Cisco products. • Cisco Jabber for Windows • Cisco IOS XR Software (if an active interface is configured under multicast routing and it is receiving DVMRP traffic) • ASR 9000 Series Aggregation Services Routers (32-bit and 64-bit models) • IOS XR, SW only • Network Convergence System 540, 560, 1000, 4000, 5000, 5500, 6000, 8000 Series • Cisco Enterprise NFVIS releases 3.5.1 through 4.1.2. • IOS XRv 9000 Router
Recommendations	NCSC-IE recommends that users apply the appropriate updates or workarounds as as recommended by Cisco as soon as possible.

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, which 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. [1] **CVE-2020-3566 (CVSS Score: Base 8.6)** This vulnerability 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 crash the IGMP process or cause memory exhaustion, resulting in other processes becoming unstable [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. 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. [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. 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 which could allow an attacker to overwrite and upload files [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 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]

[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
[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