CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-023

Critical Vulnerabilities in Cisco Products

May 6, 2021 — v1.0

TLP:WHITE

Summary

On 5th of March 2021, Cisco released several security updates to address several security flaws [1]. The list includes two critical vulnerabilities affecting Cisco SD-WAN vManage and HyperFlex HX software that could allow privilege escalation, command injection or unauthorised access to applications.

Technical Details

Critical Vulnerabilities

CVE-2021-1275, CVE-2021-1468, CVE-2021-1505

Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorised access to the application [2].

CVE-2021-1497, CVE-2021-1498

Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device [3].

Other Vulnerabilities

Additionally to the critical vulnerabilities mentioned above Cisco announced several others, most notably:

- Cisco SD-WAN Software vDaemon Denial of Service Vulnerability - SIR: High
- Cisco SD-WAN vEdge Software Buffer Overflow Vulnerabilities - SIR: High
- Cisco SD-WAN vManage Software Authentication Bypass Vulnerability - SIR: High
- Cisco AnyConnect Secure Mobility Client for Windows DLL and Executable Hijacking Vulnerabilities - SIR: High
- Cisco Enterprise NFV Infrastructure Software Command Injection Vulnerability - SIR: High
- Cisco Small Business 100, 300, and 500 Series Wireless Access Points Vulnerabilities - SIR: High

- Cisco Unified Communications Manager IM & Presence Service SQL Injection Vulnerabilities - SIR: High

Products Affected

The critical vulnerabilities affect Cisco devices if they are running a vulnerable release of Cisco SD-WAN vManage Software or a vulnerable release of Cisco HyperFlex HX Software mentioned in [3].

Recommendations

Cisco has released software updates that address these critical vulnerabilities [1, 2, 3].

There are no workarounds that address the critical 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-sd-wan-vmanage-4TbynnhZ

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR