HC3: Sector Alert

May 12, 2021 TLP: White Report: 202105121300

Severe Cisco Vulnerabilities Impact Healthcare IT

Executive Summary

On May 5, 2021 Cisco advisories disclosed multiple vulnerabilities in their products. These vulnerabilities could allow an unauthorized user to execute arbitrary code, escalate privileges and gain access to sensitive information. Many of these vulnerabilities had a severity rating of either high or critical and the technologies are known to be used in healthcare. These vulnerabilities should be carefully considered for patching by any healthcare organization with special consideration to each vulnerability criticality category against the risk management posture of the organization.

Report

Cisco disclosed 42 vulnerabilities in several of their products on May 5, 2021 addressing multiple techniques that could allow an unauthorized user to execute arbitrary code, escalate privileges and gain access to systems. The vulnerabilities are not dependent on one another - exploitation of one is not required to exploit another. Cisco highlighted detailed complications surrounding the SD-WAN software and HyperFlex HX Data Platform of which the seven critical vulnerabilities belong. An additional 17 vulnerabilities classified as high were disclosed involving products surrounding SD-WAN management, wireless access points, infrastructure for voice and video, etc. Cisco issued security updates to also address high and medium vulnerabilities that allow attackers to trigger denial of service conditions.

Analysis

The Cisco products and services that are impacted by the vulnerabilities in the advisory are widely used within healthcare organizations. Products such as Cisco vManage provides a GUI interface to make monitoring, configuring and maintaining SD-WAN devices more user friendly. The vManage platform has multiple critical and high vulnerabilities. There are also concerns of the possibility of threat actors taking advantage of conditions that could bypass authorization checks and exploit insufficient validation of user-supplied input. Threat actors can use these exploits to their advantage by targeting organizations that are slow to patch the applications.

Vulnerabilities

The table below summarizes the vulnerabilities in this advisory.

Vulnerability	Product	Impact
CVE-2021-1275	Cisco SD-WAN vManage Software	Critical
CVE-2021-1468	Cisco SD-WAN vManage Software	Critical
CVE-2021-1505	Cisco SD-WAN vManage Software	Critical
CVE-2021-1506	Cisco SD-WAN vManage Software	Critical
CVE-2021-1508	Cisco SD-WAN vManage Software	Critical

HC3: Sector Alert

May 12, 2021 TLP: White Report: 202105121300

Vulnerability	Product	Impact
CVE-2021-1497	Cisco HyperFlex HX	Critical
CVE-2021-1498	Cisco HyperFlex HX	Critical
CVE-2021-1513	Cisco SD-WAN Software	High
CVE-2021-1509	Cisco SD-WAN vEdge Software	High
CVE-2021-1510	Cisco SD-WAN vEdge Software	High
CVE-2021-1511	Cisco SD-WAN vEdge Software	High
CVE-2021-1284	Cisco SD-WAN vManage Software	High
CVE-2021-1400	Cisco Small Business 100, 300, and 500 Series Wireless Access Points	High
CVE-2021-1401	Cisco Small Business 100, 300, and 500 Series Wireless Access Points	High
CVE-2021-1421	Cisco Enterprise NFV Infrastructure Software (NFVIS)	High
CVE-2021-1363	Cisco Unified Communications Manager IM & Presence Service	High
CVE-2021-1365	Cisco Unified Communications Manager IM & Presence Service	High
CVE-2021-1426	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1427	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1428	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1429	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1430	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1496	Cisco AnyConnect Secure Mobility Client for Windows	High
CVE-2021-1490	Cisco AsyncOS for Cisco Web Security Appliance (WSA)	Medium
CVE-2021-1438	Cisco Wide Area Application Services (WAAS) Software	Medium
CVE-2021-1507	Cisco SD-WAN vManage Software	Medium
CVE-2021-1486	Cisco SD-WAN vManage Software	Medium
CVE-2021-1478	Cisco Unified Communications Manager/ Cisco Unified Communications Manager Session Management Edition (Unified CM SME)	Medium
CVE-2021-1532	Cisco TelePresence Collaboration Endpoint (CE) Software/ Cisco RoomOS Software	Medium
CVE-2021-1447	Cisco Content Security Management Appliance	Medium
CVE-2021-1234	Cisco SD-WAN vManage Software	Medium
CVE-2021-1535	Cisco SD-WAN vManage	Medium
CVE-2021-1514	Cisco SD-WAN Software	Medium
CVE-2021-1515	Cisco SD-WAN vManage Software	Medium
CVE-2021-1520	Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	Medium
CVE-2021-1521	Cisco Video Surveillance 8000 Series IP Cameras	Medium
CVE-2021-1397	Cisco Integrated Management Controller (IMC) Software	Medium
CVE-2021-1499	Cisco HyperFlex HX Data Platform	Medium
CVE-2021-1516	Cisco Content Security Management Appliance, Email Security Appliance, and Web Security Appliance	Medium
CVE-2021-1530	Cisco BroadWorks Messaging Server Software	Medium
CVE-2021-1519	Cisco AnyConnect Secure Mobility Client	Medium
CVE-2020-3347	Cisco Webex Meetings Desktop App for Windows	Medium

HC3: Sector Alert

May 12, 2021 TLP: White Report: 202105121300

Patches, Mitigations & Workarounds:

HC3 strongly recommends healthcare organizations update applicable Cisco products and services. It is highly advised to patch reported vulnerabilities to protect systems against possible exploits. When patches can't be immediately applied, proper mitigation actions can be a viable temporary solution. Vulnerabilities should be triaged and prioritized for patching by healthcare organizations with special consideration to each vulnerability criticality category against the risk management posture of the enterprise. For detailed information about which Cisco products and services are vulnerable, see Cisco Security Advisories. It's also recommended that any healthcare organization that operates Cisco products as part of their enterprise architecture periodically monitors the Cisco advisory page for new releases, as they often occur multiple times each month.

References

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x

Critical Cisco SD-WAN, HyperFlex Bugs Threaten Corporate Networks
https://threatpost.com/critical-cisco-sd-wan-hyperflex-bugs/165923/

Cisco publishes solutions to SD-WAN and HyperFlex software security vulnerabilities
https://www.zdnet.com/article/cisco-publishes-solutions-to-sd-wan-and-hyperflex-software-security-vulnerabilities/

Cisco bugs allow creating admin accounts, executing commands as root
https://www.bleepingcomputer.com/news/security/cisco-bugs-allow-creating-admin-accounts-executing-commands-as-root/

Critical Flaws Hit Cisco SD-WAN vManage and HyperFlex Software
https://thehackernews.com/2021/05/critical-flaws-hit-cisco-sd-wan-vmanage.html

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback