KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cisco releases security patches for high-severity vulnerabilities

Tracker ID: TN0912 **Date:** 12/Sep/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Three security issues affecting Cisco products were recently addressed, including a high-severity vulnerability identified late last month in the NVIDIA Data Plane Development Kit (MLNX DPDK). The vulnerability CVE-2022-28199 (CVSS score: 8.6) is caused by improper error handling in the DPDK network stack, allowing a remote attacker to cause a denial-of-service (DoS) condition and compromise data integrity and confidentiality.

The DPDK suite of libraries and network interface card (NIC) drivers provides a framework and standard API for high-speed networking applications. If an error condition on the device interface is met, the device may reload or cease receiving traffic, resulting in a denial-of-service (DoS). Cisco has confirmed that the following Cisco products are not affected by this vulnerability: Cloud Services Router 1000V Series, IOS Software, IOS XE Software (other than Cisco Catalyst 8000V Edge Software), IOS XR Software, and NX-OS Software.

In addition to CVE-2022-28199, Cisco has patched a vulnerability in its SD-WAN vManage software that might allow an unauthenticated attacker to access an affected device's VPN0 logical network and messaging service ports. CVE-2022-20696 (CVSS score: 7.5) was assigned to the vulnerability due to a lack of "adequate protective mechanisms" in the message server container ports. If the vulnerability is successfully exploited, the attacker may be able to see and insert messages into the messaging service, potentially modifying configuration settings or necessitating a system reload.

Cisco also patched a vulnerability in the messaging interface of the Cisco Webex App (CVE-2022-20863, CVSS score: 4.3), which might allow a remote, unauthenticated attacker to modify links or other content and launch phishing attacks. This flaw exists because of how the impacted program handles character rendering. An attacker could exploit this vulnerability by sending messages through the application interface.

Lastly, an authentication bypass vulnerability (CVE-2022-20923, CVSS score: 4.0) that impacts Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers, will not be patched due to the products' near-end-of-life status (EOL). Customers are urged to "upgrade to Cisco Small Business RV132W, RV160, or RV160W Routers" since "Cisco has not issued and will not release software upgrades to address the vulnerability.“

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-28199	High	8.6
CVE-2022-20696	High	7.5
CVE-2022-20863	Medium	4.3
CVE-2022-20923	Medium	4.0

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cisco releases security patches for high-severity vulnerabilities

Tracker ID: TN0912 **Date:** 12/Sep/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Affected Products and Versions

- Cisco Catalyst 8000V Edge Software version 17.6, 17.7 and 17.8.
- Adaptive Security Virtual Appliance (ASAv) version 9.17 and 9.18.
- Secure Firewall Threat Defense Virtual (formerly FTDv) version 7.1 and 7.2.

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.
- Update application to its patched version as mentioned below.
  - Cisco Catalyst 8000V Edge Software : 17.6.4, 17.7.2,17.9.1 and later.
  - Adaptive Security Virtual Appliance (ASAv) : 9.17.1.x (release date TBD), 9.18.2, 9.19.x and later
  - Secure Firewall Threat Defense Virtual (formerly FTDv) : 7.1.0.3-x (release date TBD), 7.2.1.x (release date TBD), 7.3.x and later.

References

- Ravie Lakshmanan, Cisco Releases Security Patches for New Vulnerabilities Impacting Multiple Products, Hacker News, 08th September 2022, External Link (thehackernews.com)
- Vulnerability in NVIDIA Data Plane Development Kit Affecting Cisco Products: August 2022, Cisco, 07th September 2022, External Link (tools.cisco.com)
- Security Bulletin: NVIDIA Data Plane Development Kit (MLNX_DPDK) - August 2022, NVIDIA, 29th August 2022, External Link (nvidia.custhelp.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia