KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cisco Fixes Multiple Vulnerabilities in IOS and IOS XE Products

Tracker ID: TN2350 **Date:** March 24, 2023 **Category:** Vulnerability **Industry:** Technology **Region**: All

Background

The semi-annual IOS and IOS XE software security advisory from Cisco released this week addresses ten vulnerabilities. Six of which are classified as high severity. The three identified security flaws could allow remote unauthenticated attackers to create a denial-of-service (DoS) condition. The high vulnerability tracked as CVE-2023-20080 affects the IPv6 DHCP version 6 (DHCPv6) relay and server functionality of IOS and IOS XE software. An attacker could send customized DHCPv6 signals to a vulnerable device that could trigger an unexpected restart due to insufficient data boundary validation. Cisco has released the free software updates to address the vulnerability.

The second flaw, CVE-2023-20072, affects tunnel protocol packets handle fragmentation and could be exploited by sending specially crafted fragmented packets to a vulnerable system. CVE-2023-20027, a vulnerability with the implementation of the IPv4 Virtual Fragmentation Reassembly (VFR) feature of IOS and IOS XE software, arises as big packets are not correctly reassembled when VFR is enabled. Sending fragmented packets across a VFR-enabled interface on an affected device could lead to the exploitation of the vulnerability.

In the HTTP-based client profiling function of the IOS XE software for Wireless LAN controllers, another serious DoS issue was fixed. The vulnerability, identified as CVE-2023-20067, could be abused by a nearby attacker without authentication. This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by using a wireless access point to send specially created traffic. A successful exploit could enable the attacker to raise CPU usage, which could lead to a DoS condition on a vulnerable device and failure of new wireless client associations.

Cisco fixed another bug that could have allowed an authenticated attacker to run commands with root-level access on the operating system in the CLI of the IOS XE SD-WAN software. Tracked as CVE-2023-20035, the bug could allow an attacker with limited privileges to take over a vulnerable system. The IOx application hosting subsystem of the IOS XE software contained, a high-severity flaw tracked as CVE-2023-20065, that could also allow an authenticated attacker to gain root privileges.

Apart from the above-mentioned high severity flaws, Cisco also released patches for medium-severity DoS, path traversal, and privilege escalation vulnerabilities semi-annual IOS and IOS XE software upgrades. Several medium-severity issues were resolved in SD-WAN vManage software, DNA Center, Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), IOS and IOS XE software, and AP software. Administrators are advised to identify the vulnerable Cisco products in the network and implement the patch as soon as possible.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cisco Fixes Multiple Vulnerabilities in IOS and IOS XE Products

Analysis

CVE ID	Severity	CVSS Score
CVE-2023-20080	High	8.6
CVE-2023-20072	High	8.6
CVE-2023-20027	High	8.6
CVE-2023-20035	High	7.8
CVE-2023-20065	High	7.8
CVE-2023-20067	High	7.4

Affected Products and Versions

- **CVE-2023-20080:** affects Cisco devices if they are running a vulnerable release of Cisco IOS or IOS XE Software and have IPv6 and the DHCPv6 relay or server feature enabled. Note: IPv6 and DHCPv6 are disabled in Cisco IOS and IOS XE Software by default.
- **CVE-2023-20072:** affects Cisco products if they are running Cisco IOS XE Software releases 17.9.1, 17.9.1a, or 17.9.1w and have a tunnel interface configured.
- **CVE-2023-20027:** affects the following Cisco products if they are running a vulnerable release of Cisco IOS XE Software and have the VFR feature enabled:
    - 1000 Series Integrated Services Routers
    - 4000 Series Integrated Services Routers
    - Catalyst 8000V Edge Software Routers
    - Catalyst 8200 Series Edge Platforms
    - Catalyst 8300 Series Edge Platforms
    - Catalyst 8500L Series Edge Platforms
    - Cloud Services Router 1000V Series

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cisco Fixes Multiple Vulnerabilities in IOS and IOS XE Products

- **CVE-2023-20035**: affects the following Cisco products if they are running a vulnerable release of universal Cisco IOS XE Software in controller mode or a vulnerable release of standalone Cisco IOS XE SD-WAN Software:
    - 1000 Series Integrated Services Routers (ISRs)
    - 4000 Series ISRs
    - ASR 1000 Series Aggregation Services Routers
    - Catalyst 8000 Edge Platforms Family
    - Cloud Services Router (CSR) 1000V Series.
- **CVE-2023-20065:** affects Cisco products if they are running a vulnerable release of Cisco IOS XE Software, they have the Cisco IOx application hosting feature configured, and the hosted application is running. Note: Cisco IOx application hosting infrastructure is not enabled by default.
- **CVE-2023-20067:** affects the following Cisco products if they are running a vulnerable release of Cisco IOS XE Software for WLCs and have the HTTP-based client profiling feature configured. Note: Client profiling is not enabled by default.
    - Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches
    - Catalyst 9800 Series Wireless Controllers
    - Catalyst 9800-CL Wireless Controllers for Cloud
    - Embedded Wireless Controllers on Catalyst Access Points

Recommendations

- Administrators are advised to immediately identify the vulnerable instances and apply the latest vendor-provided patch shared in the Cisco Advisory security updates.

References

- Cisco Event Response: March 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication, CISCO, March 23, 2023, External Link (cisco.com)
- ByIonut Arghire, Cisco Patches High-Severity Vulnerabilities in IOS Software, Security Week, March 23, 2023, External Link (securityweek.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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia