Cisco patches IOS XE zero-days used to hack over 50,000 devices

By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

October 23, 2023 10:08 AM **0**

Cisco has addressed the two vulnerabilities (CVE-2023-20198 and CVE-2023-20273) that hackers exploited to compromise tens of thousands of IOS XE devices over the past week.

The free software release comes after a threat actor leveraged the security issues as zero-days to compromise and take full control of more than 50,000 Cisco IOS XE hosts.

Critical and medium-severity flaws

In an update to the original advisory, Cisco says that the first fixed software release is available from the company's Software Download Center (https://software.cisco.com/download/home).

At the moment, the first fixed release available is 17.9.4a, with updates to roll out at a yet undisclosed date.

Cisco IOS XE Software Release Train	First Fixed Release	Available
17.9	17.9.4a	Yes
17.6	17.6.6a	TBD
17.3	17.3.8a	TBD
16.12 (Catalyst 3650 and 3850 only)	16.12.10a	TBD

Both vulnerabilities, which Cisco tracks as CSCwh87343 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh87343), are in the web UI of Cisco devices running the IOS XE software. CVE-2023-20198 has the maximum severity rating (10/10) while CVE-2023-20273 has been assigned a high severity score of 7.2.

The vendor of networking gear says that the threat actor exploited the critical flaw to gain initial access to the device and then "issued a privilege 15 command" to create a normal local account.

On Cisco devices, permissions to issue commands are locked into levels from zero to 15, with zero providing five basic commands ("logout," "enable," "disable," "help," and "exit") and 15 being the most privileged level that provides complete control over the device.

By leveraging CVE-2023-20273, the attacker elevated to root the privileges of the new local user and added a malicious script to the file system. The implant does not provide persistence and a reboot will remove it from the system.

The company warns that the two vulnerabilities can be exploited if the web UI (HTTP Server) feature of the device is turned on, which is possible through the *ip http server* or *ip http secure-server* commands.

Administrators can check if the feature is active by running the *show running-config | include ip http server|secure|active* command to check in the global configuration for the *ip http server* or the *ip http secure-server* Commands.

> “The presence of either command or both commands in the system configuration indicates that the web UI feature is enabled” - Cisco (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z)

Sudden drop in Hacked Cisco IOS XE hosts

When Cisco disclosed CVE-2023-20198 (https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-ios-xe-zero-day-actively-exploited-in-attacks/) on October 16 as a zero-day exploited in the wild, security researchers started looking for compromised devices.

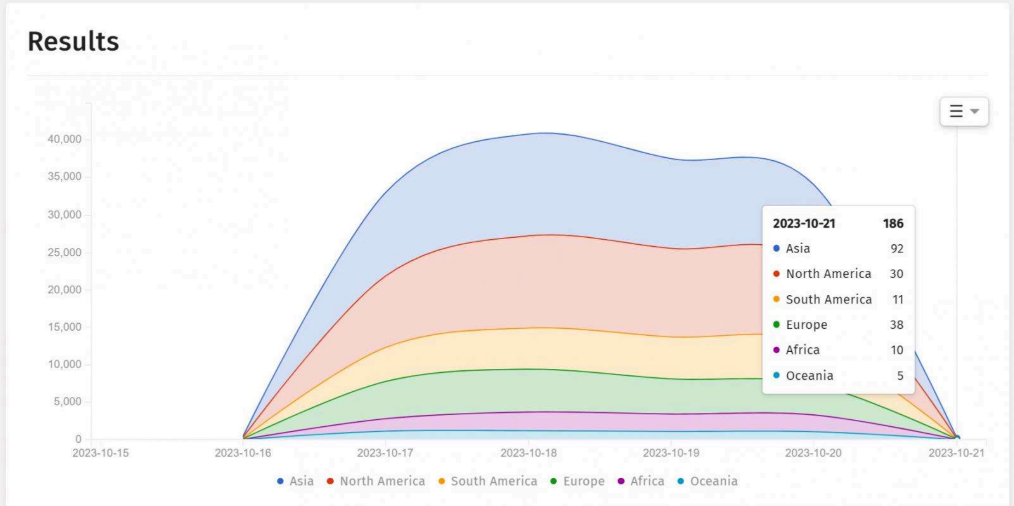
Initial findings estimated that about 10,000 Cisco IOS XE vulnerable devices had been infected (https://www.bleepingcomputer.com/news/security/over-10-000-cisco-devices-hacked-in-ios-xe-zero-day-attacks/) by Tuesday. The number grew quickly to more than 40,000 (https://www.bleepingcomputer.com/news/security/over-40-000-cisco-ios-xe-devices-infected-with-backdoor-using-zero-day/) in just a few days as more researchers joined the search.

On October 20, Cisco disclosed the second zero-day (https://www.bleepingcomputer.com/news/security/cisco-discloses-new-ios-xe-zero-day-exploited-to-deploy-malware-implant/) being exploited in the same campaign to take complete control of systems running the IOS XE software.

Over the weekend, though, researchers saw a steep drop in the number of Cisco IOS XE hosts hacked using the two zero-day vulnerabilities, from about 60,000 to just a few hundred (https://www.bleepingcomputer.com/news/security/number-of-hacked-cisco-ios-xe-devices-plummets-from-50k-to-hundreds/).

It is unclear what caused the mysterious sudden drop but one theory is that the attacker has deployed an update to hide their presence and the malicious implants are no longer visible in scans.

Piotr Kijewski, the CEO of The Shadowserver Foundation told BleepingComputer that they observed a sharp drop in implants since October 21 to just 107 devices.



Count of hacked Cisco IOS XE devices plummets
source: The ShadowServer Foundation (https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=7&source=compromised_website&source=compromised_website6&tag=device-implant%2B&group_by=geo&style=stacked)

The reason for the sudden low number could also be that a grey-hat hacker has been automatically rebooting infected devices to remove the malicious implant.

However, we can't know for sure until Cisco completes its investigation and provides a public report or other security researchers come to a conclusion analyzing a breached Cisco IOS XE system.

After publishing this article, researchers at Fox-IT cybersecurity company published new information that explains why the number of compromised Cisco IOS XE devices plumetted lately.

Fox-IT says that the malicious code on tens of thousands of devices "has been altered to check for an Authorization HTTP header value before responding" and that using a different method shows that 37,890 are still compromised.

The researchers advise admins with IOS XE systems that have the web UI exposed on the internet to do a forensic triage and provide a repository with the necessary steps to check if the implant was active on the host (https://github.com/fox-it/cisco-ios-xe-implant-detection).

They repository also provides an alternative method to scan devices for the presence of the malicious code planted during the Cisco IOS XE hack campaign.

Update [12:16 PM, EDT]: *Added information from Fox-IT researchers saying that hacked Cisco IOS XE devices are no longer visible because the malicious implant on them has been modified to*