Over 10,000 Cisco devices hacked in IOS XE zero-day attacks

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** October 17, 2023 09:15 AM **0**

Update October 17, 16:40 EDT: Added new information on breached Cisco IOS XE devices.

Update October 18, 05:06 EDT: Orange Cyberdefense CERT discovered (https://twitter.com/CERTCyberdef/status/1714567941184749609) over 34.5K Cisco IOS XE devices compromised in CVE-2023-20198 attacks.

Attackers have exploited a recently disclosed critical zero-day bug to compromise and infect over 10,000 Cisco IOS XE devices with malicious implants.

The list of products running Cisco IOS XE software includes enterprise switches, aggregation and industrial routers, access points, wireless controllers, and more.

According to threat intelligence company VulnCheck, the maximum severity vulnerability (CVE-2023-20198) has been extensively exploited in attacks targeting Cisco IOS XE systems with the Web User Interface (Web UI) feature enabled, that also have the HTTP or HTTPS Server feature toggled on.

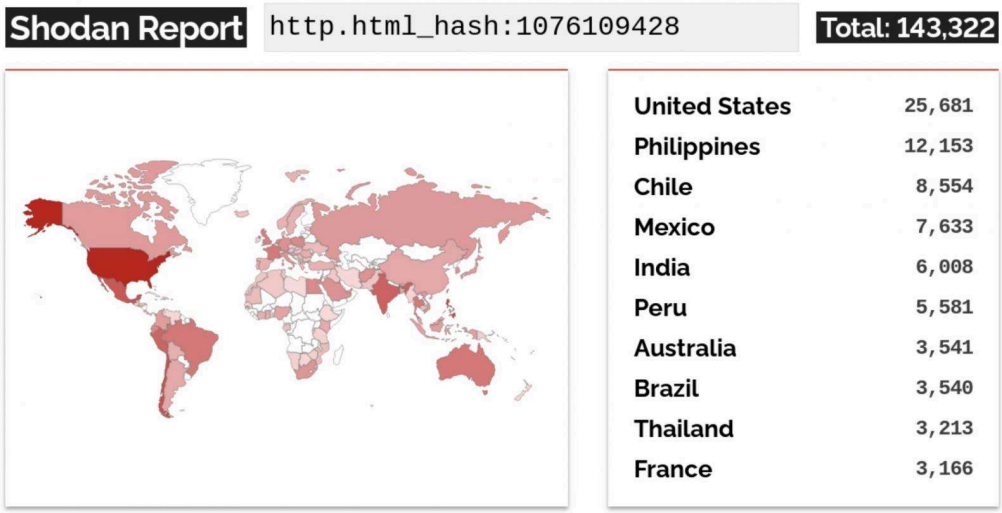
VulnCheck scanned internet-facing Cisco IOS XE web interfaces and discovered thousands of infected hosts. The company has also released a scanner to detect these implants on affected devices.

"Cisco buried the lede by not mentioning *thousands* of internet-facing IOS XE systems have been implanted. This is a bad situation, as privileged access on the IOS XE likely allows attackers to monitor network traffic, pivot into protected networks, and perform any number of man-in-the-middle attacks," said VulnCheck CTO Jacob Baines (https://vulncheck.com/blog/cisco-implants).

"If your organization uses an IOS XE system, it's imperative that you determine if your systems have been compromised and take appropriate action once implants have been discovered. While a patch is not yet available, you can protect your organization by disabling the web interface and removing all management interfaces from the internet immediately."

"*VulnCheck has fingerprinted approximately 10,000 implanted systems*, but we've only scanned approximately half of the devices listed on Shodan/Censys. We didn't want to commit to a specific number as it's evolving (increasing) as we continue our activities," Baines told BleepingComputer.

A Shodan search for Cisco devices with their Web UI enabled (shared (https://twitter.com/SimoKohonen/status/1714213806371479849) by Aves Netsec CEO Simo Kohonen) currently shows more than 140,000 Internet-exposed devices.



Internet-exposed Cisco devices with Web UI enabled (Shodan)

Cisco: Apply mitigation measures and look for breach indicators

On Monday, Cisco disclosed that unauthenticated attackers can exploit the IOS XE zero-day (https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-ios-xe-zero-day-actively-exploited-in-attacks/) to gain full administrator privileges and take complete control over affected Cisco routers and switches remotely.

The company cautioned administrators to disable the vulnerable HTTP server feature on all internet-facing systems until a patch becomes available.

Cisco detected the CVE-2023-20198 attacks in late September following reports of unusual behavior on a customer device received by Cisco's Technical Assistance Center (TAC). Evidence of these attacks dates back to September 18, when the attackers were observed creating local user accounts named "cisco_tac_admin" and "cisco_support."

Moreover, the attackers deployed malicious implants using CVE-2021-1435 exploits and other unknown methods, enabling them to execute arbitrary commands at the system or IOS levels on compromised devices.

"We assess that these clusters of activity were likely carried out by the same actor. Both clusters appeared close together, with the October activity appearing to build off the September activity,"

Cisco said.

"The first cluster was possibly the actor's initial attempt and testing their code, while the October activity seems to show the actor expanding their operation to include establishing persistent access via deployment of the implant."

The company also issued a "strong recommendation" for administrators to look for suspicious or recently created user accounts as potential signs of malicious activity linked to this threat.

In September, Cisco cautioned customers to patch another zero-day vulnerability (https://www.bleepingcomputer.com/news/security/cisco-urges-admins-to-fix-ios-software-zero-day-exploited-in-attacks/) (CVE-2023-20109) in its IOS and IOS XE software, targeted by attackers in the wild.

Related Articles:

Malicious ads exploited Internet Explorer zero day to drop malware (https://www.bleepingcomputer.com/news/security/malicious-ads-exploited-internet-explorer-zero-day-to-drop-malware/)

Google: 70% of exploited flaws disclosed in 2023 were zero-days (https://www.bleepingcomputer.com/news/security/google-70-percent-of-exploited-flaws-disclosed-in-2023-were-zero-days/)

Mozilla fixes Firefox zero-day actively exploited in attacks (https://www.bleepingcomputer.com/news/security/mozilla-fixes-firefox-zero-day-actively-exploited-in-attacks/)

Ivanti warns of three more CSA zero-days exploited in attacks (https://www.bleepingcomputer.com/news/security/ivanti-warns-of-three-more-csa-zero-days-exploited-in-attacks/)

Qualcomm patches high-severity zero-day exploited in attacks (https://www.bleepingcomputer.com/news/security/qualcomm-patches-high-severity-zero-day-exploited-in-attacks/)