Over 40,000 Cisco IOS XE devices infected with backdoor using zero-day

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

October 19, 2023 09:08 PM **0**

More than 40,000 Cisco devices running the IOS XE operating system have been compromised after hackers exploited a recently disclosed maximum severity vulnerability tracked as CVE-2023-20198.

There is no patch or a workaround available and the only recommendation for customers to secure the devices is to “disable the HTTP Server feature on all internet-facing systems.”

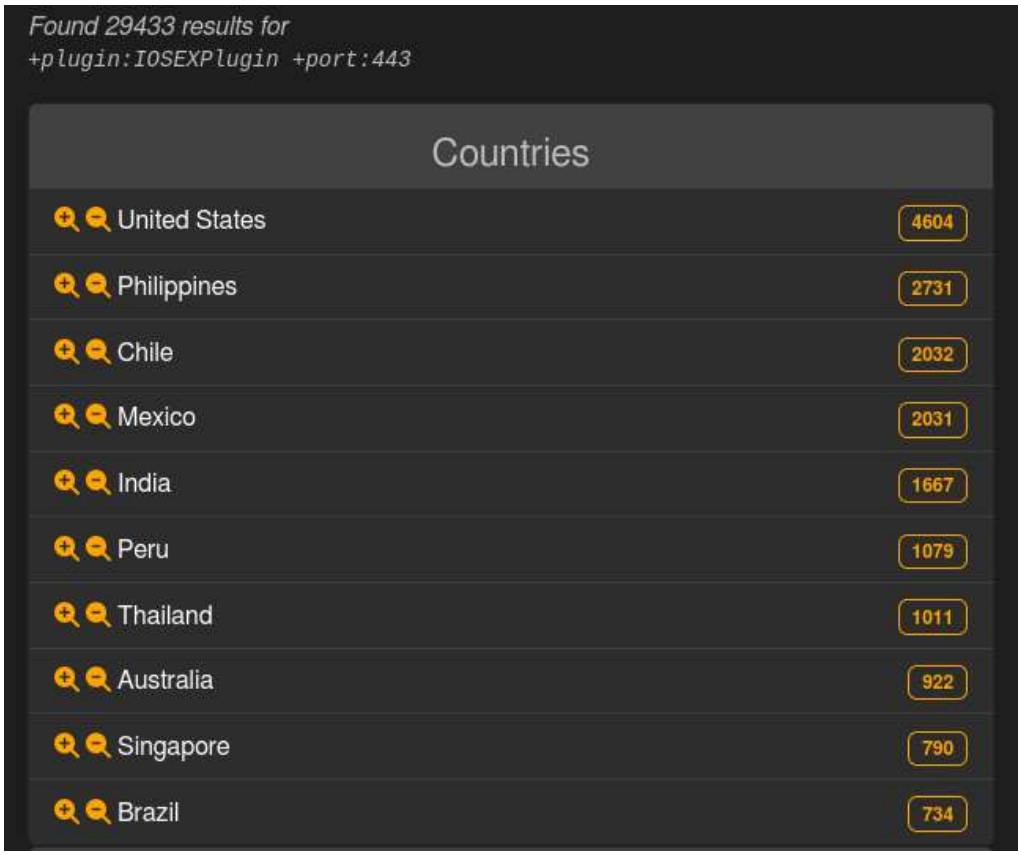
Networking gear running Cisco IOS XE includes enterprise switches, industrial routers, access points, wireless controllers, aggregation, and branch routers.

Tens of thousands of Cisco devices exposed

Initial estimates of breached Cisco IOS XE devices were around 10,000 (https://www.bleepingcomputer.com/news/security/over-10-000-cisco-devices-hacked-in-ios-xe-zero-day-attacks/)and the number started growing as security researchers scanned the internet for a more accurate figure.

On Tuesday, the LeakIX engine for indexing services and web applications exposed on the public web said they found about 30,000 infected devices, without counting the rebooted systems.

The search relied on the indicators of compromise (IoCs) that Cisco provided to determine the successful exploitation of CVE-2023-20198 on an exposed device and revealed thousands of infected hosts in the United States, the Philippines, and Chile.



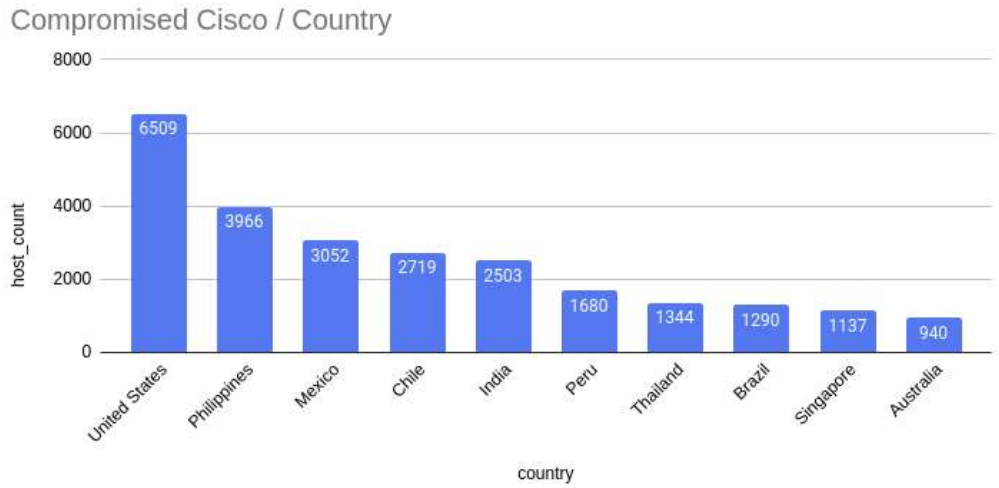
LeakIX results for Cisco IOS XE devices exposed online

source: LeakIX (https://twitter.Com/leak_ix/status/1714342183141028307)

Using the same verification method from Cisco, the private CERT from Orange announced on Wednesday that there were more than 34,500 Cisco IOS XE IP addresses (https://twitter.com/CERTCyberdef/status/1714567941184749609) with a malicious implant as a result of exploiting CVE-2023-20198.

CERT Orange also published a Python script (https://github.com/cert-orangecyberdefense/Cisco_CVE-2023-20198) to scan for the presence of a malicious implant on a network device running Cisco IOS XE.

In an update on October 18 (https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/), the Censys search platform for assessing attack surface for internet-connected devices said that the number of compromised devices it found increased to 41,983.



Censys results for Cisco IOS XE hosts on the public web

source: Censys

A precise number of Cisco IOS XE devices reachable over the public internet is difficult to obtain but Shodan shows a little over 145,000 hosts, most of them in the U.S.

Below is a screenshot with Shodan results for Cisco devices that have their Web UI accessible over the internet, using a query from Simo Kohonen, the CEO of Aves Netsec cybersecurity company.

Shodan results for exposed Cisco IOS XE systems
source: BleepingComputer

Yutaka Sejiyama (https://twitter.com/nekono_naha), a security researcher at Macnica, also searched Shodan for Cisco IOS XE devices vulnerable to CVE-2023-20198 and found close to 90,000 hosts exposed on the web.

In the U.S., many of the devices are from communications providers such as Comcast, Verizon, Cox Communications, Frontier, AT&T, Spirit, CenturyLink, Charter, Cobridge, Windstream, and Google Fiber.

Sejiyama's list also includes medical centers, universities, sheriff's offices, school districts, convenience stores, banks, hospitals, and government entities with Cisco IOS XE devices exposed online.

"There is no need to expose the IOS XE login screen on the Internet in the first place," Sejiyama told BleepingComputer, echoing Cisco's advice of not exposing the web UI and management services to the public web or to untrusted networks.

The researcher expressed concern at this practices, saying that "organizations using the equipment in such a manner are likely to be unaware of this vulnerability or breach."

Risk persists after device reboot

Cisco disclosed CVE-2023-20198 on Monday but threat actors had been leveraging it before September 28, when it was a zero-day, to create a high-privilege account on affected hosts and take full control of the device.

Cisco updated its advisory (https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/) today with new attacker IP addresses and usernames, as well as fresh rules for the Snort open-source network intrusion detection system and intrusion prevention system.

The researchers note that threat actors behind these attacks use a malicious implant, which does not have persistence and is removed after rebooting the device.

However, the new accounts it helped create continue to be active and “have level 15 privileges, meaning they have full administrator access to the device.”

Based on Cisco’s analysis, the threat actor collects details about the device and carries out preliminary reconnaissance activity. The attacker is also clearing logs and removing users, probably to hide their activity.

The researchers believe that behind these attacks is only one threat actor but could not determine the initial delivery mechanism.

Cisco has not disclosed additional details about the attacks but promised to offer more information when it completes the investigation and when a fix is available.

Related Articles:

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/)

Microsoft October 2024 Patch Tuesday fixes 5 zero-days, 118 flaws (https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2024-patch-tuesday-fixes-5-zero-days-118-flaws/)

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

CISA: Network switch RCE flaw impacts critical infrastructure (https://www.bleepingcomputer.com/news/security/cisa-network-switch-rce-flaw-impacts-critical-infrastructure/)

0DAY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/0DAY/)

CISCO (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CISCO/)

CISCO IOS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CISCO-IOS/)

ROUTER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ROUTER/)

SWITCH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SWITCH/)

VULNERABILITY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VULNERABILITY/)

WIRELESS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WIRELESS/)

ZERO-DAY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ZERO-DAY/)