Hackers update Cisco IOS XE backdoor to hide infected devices

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)**

October 22, 2023 01:37 PM **2**

10/23/23 update added at the end explaining the cause of decreased detections.

The number of Cisco IOS XE devices detected with a malicious backdoor implant has plummeted from over 50,000 impacted devices to only a few hundred after the attackers updated the backdoor to hide infected systems from scans.

This week, Cisco warned that hackers (https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-ios-xe-zero-day-actively-exploited-in-attacks/) exploited two zero-day vulnerabilities

(https://www.bleepingcomputer.com/news/security/cisco-discloses-new-ios-xe-zero-day-exploited-to-deploy-malware-implant/), CVE-2023-20198 (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z) and CVE-2023-20273, to hack over 50,000 Cisco IOS XE devices to create privileged user accounts and install a malicious LUA backdoor implant.

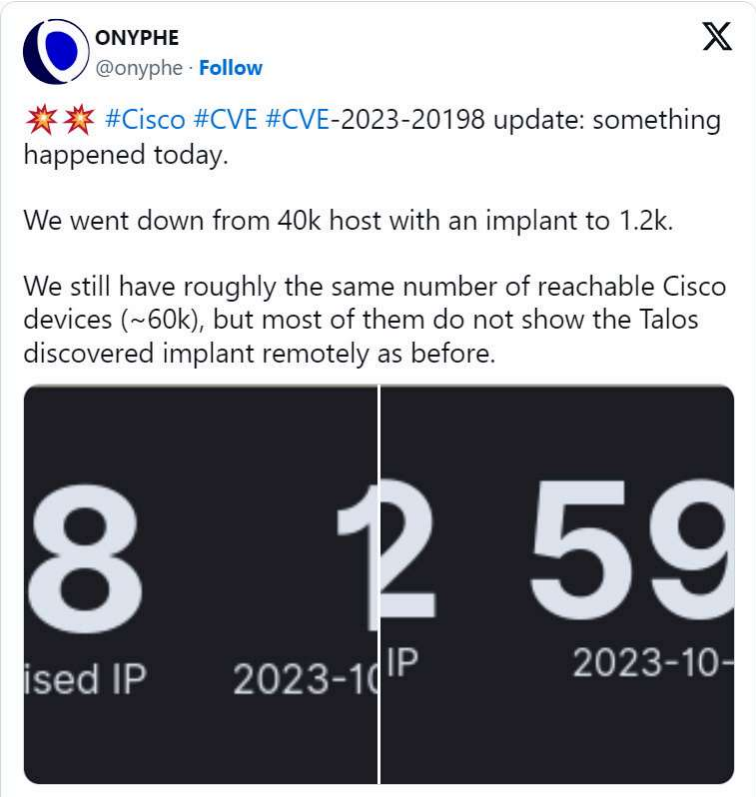
This LUA implant allows the threat actors to remotely execute commands at privilege level 15 (https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/), the highest privilege level on the device.

However, this implant does not include persistence, meaning a reboot will remove the backdoor. However, any local users created during the attack will remain.

Since the release of this news, cybersecurity firms and researchers have found roughly 60,000 out of the 80,000 publicly exposed Cisco ISO XE devices to be breached with this implant.

Mysterious drop in detected Cisco implants

On Saturday, multiple cybersecurity organizations reported that the number of Cisco IOS XE devices with a malicious implant has mysteriously dropped from approximately 60,000 devices to only 100-1,200, depending on the different scans.



(https://twitter.com/onyphe/status/1715633541264900217)

Onyphe Founder & CTO Patrice Auffret told BleepingComputer that he believes the threat actors behind the attacks are deploying an update to hide their presence, thus causing the implants to be no longer seen in scans.

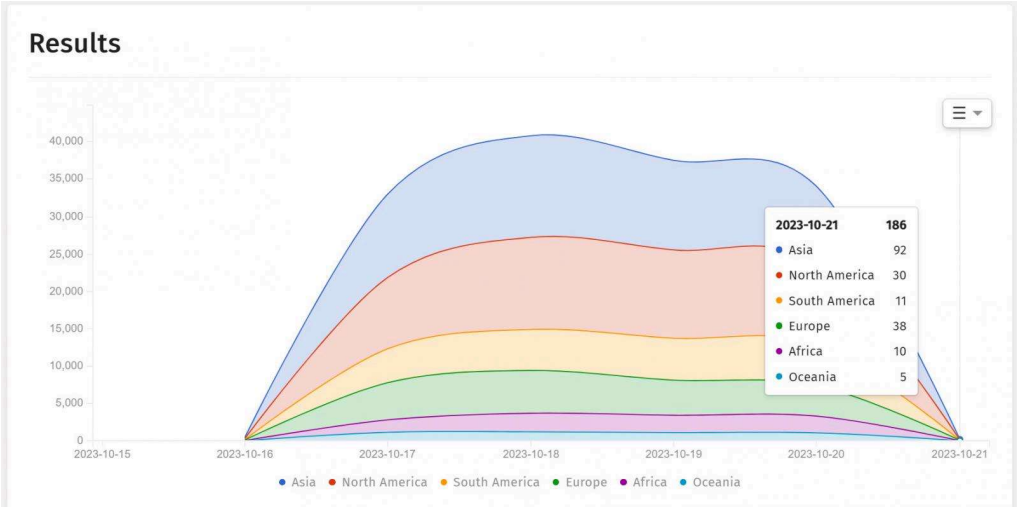
"For the second day in a row, we see the number of implants have drastically dropped in a short time (see screenshots attached). Basically, they appear to have been practically all rebooted (as the known implant doesn't survive a reboot) or have been updated."

"We believe it is the action from the original threat actor which is trying to fix an issue that should not have been there from the beginning. The fact that the implant was so easy to detect remotely was a mistake from their side.

"They are probably deploying an update to hide their presence."

Piotr Kijewski, the CEO of The Shadowserver Foundation, also told BleepingComputer that they have seen a sharp drop in implants since 10/21, with their scans only seeing 107 devices with the malicious implant.

"The implant appears to have been either removed or updated in some way," Kijewski told BleepingComputer via email.



Number of Cisco IOS XE devices with malicious implant

Source: ShadowServer (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)

Another theory shared is that a grey-hat hacker is automating the reboot of impacted Cisco IOS XE devices to clear the implant. A similar campaign was seen in 2018 (https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers/) when a hacker claimed to have patched 100,000 MikroTik routers so they could not be abused for cryptojacking and DDoS campaigns.

However, Orange Cyberdefense CERT for the Orange Group told BleepingComputer that they do not believe that a grey-hat hacker is behind the decrease in implants but rather that this could be a new exploitation phase.

"Please note that a potential trace cleaning step is underway to hide the implant (following exploitation of #CVE-2023-20198)," tweeted Orange Cyberdefense CERT (https://twitter.com/CERTCyberdef/status/1715787627800969374).

"Even if you have disabled your WebUI, we recommend that you carry out an investigation to make sure that no malicious users has been added and that its configuration has not been altered."

Finally, security researcher Daniel Card (https://twitter.com/uk_daniel_card/status/1716131549945430356?s=46) theorized that the many devices breached with implants were simply a decoy to hide the real targets in attacks.

Unfortunately, at the time, all we have are theories as to what caused the reduced detections.

Update 10/23/23: Today, cybersecurity firm Fox-IT explained that the cause of the sudden drop of detected implants is due to the threat actors rolling out a new version of the backdoor on Cisco IOS XE devices.

According to Fox-IT the new implant version now checks for an Authorization HTTP header before responding.

"We have observed that the implant placed on tens of thousands of Cisco devices has been altered to check for an Authorization HTTP header value before responding," reads the LinkedIn post (https://www.linkedin.com/feed/update/urn:li:activity:7122238350849150976/).

As the previous scan methods did not utilize an authorization header, there was no response from the implant, making it appear as if it had been removed.

Cisco Talos confirmed the change in updated advisories [1 (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z), 2 (https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/)], sharing a new curl command that can detect the implant on backdoored Cisco ISO XE devices.

This command is the same as the previously shared method but now includes an 'Authorization' header to cause the implant to respond to requests:

```
curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "https[:]//DEVICEIP/webui/logoutconfirm.html?logon_hash=1"
```

The DEVICEIP placeholder should be replaced with the device's IP address you want to check for the implant.

Once the researchers switched to using the new 'Authorization' header, scans showed that there are now 37,890 Cisco ISO XE devices infected with the malicious backdoor implant.

Related Articles:

Cisco warns of backdoor admin account in Smart Licensing Utility (https://www.bleepingcomputer.com/news/security/cisco-warns-of-backdoor-admin-account-in-smart-licensing-utility/)

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/)

Cisco investigates breach after stolen data for sale on hacking forum (https://www.bleepingcomputer.com/news/security/cisco-investigates-breach-after-stolen-data-for-sale-on-hacking-forum/)

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/)

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

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

CVE-2023-20198 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CVE-2023-20198/)

CVE-2023-20273 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CVE-2023-20273/)

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

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

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

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