Exploit released for critical Cisco IOS XE flaw, many hosts still hacked

By **Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)** October 30, 2023 11:09 PM **0**

Public exploit code is now available for the critical Cisco IOS XE vulnerability tracked as CVE-2023-20198 that was leveraged as a zero-day to hack tens of thousands of devices.

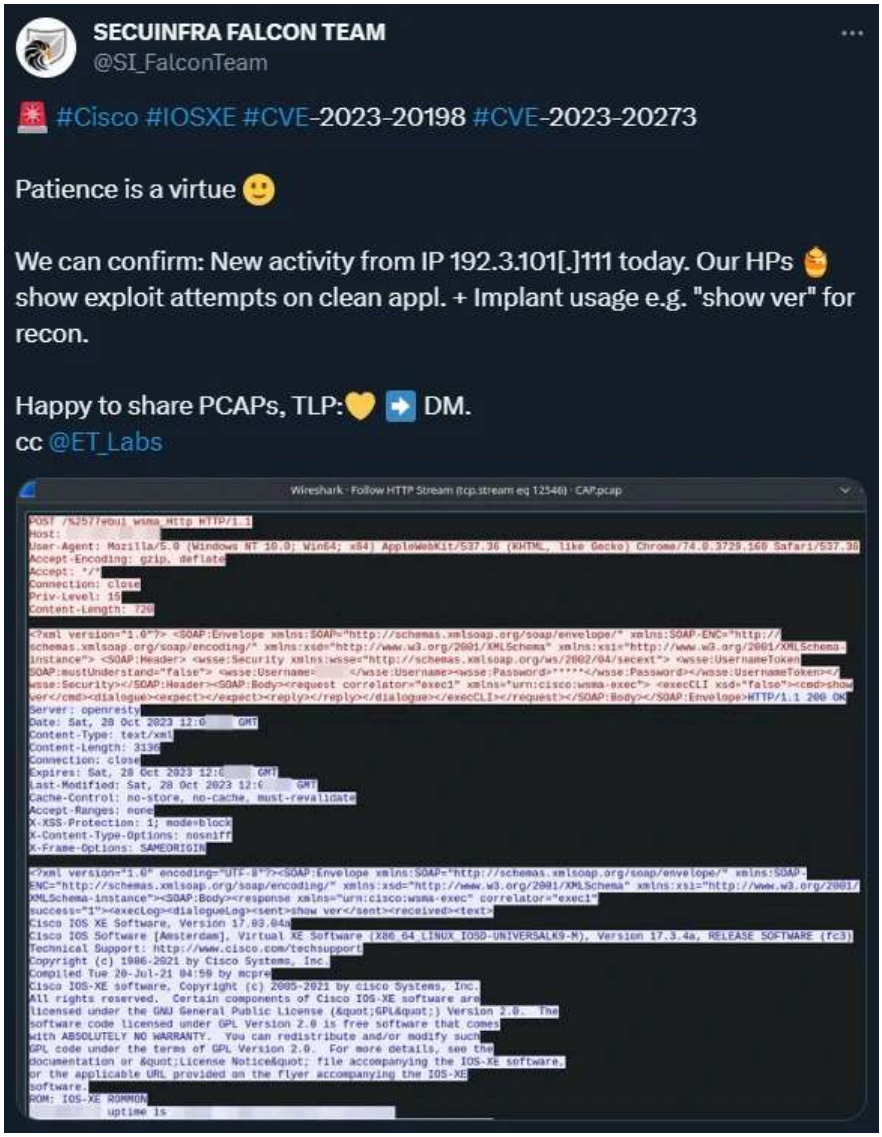
Cisco released patches for most releases of its IOS XE software but thousands of systems continue to be compromised, internet scans show.

CVE-2023-20198 exploit details

Researchers at Horizon3.ai, a company providing security assessment services, have shared details on how an attacker can bypass authentication on Cisco IOS XE devices vulnerable to CVE-2023-20198.

In a technical report (https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-deep-dive-and-poc/) today, the researchers show how hackers can exploit the maximum severity security issue to create a new user with level 15 privileges that provide complete control over the device.

The creation of the exploit was possible using information captured from a from a honeypot set up by SECUINFRA's team (https://twitter.com/SI_FalconTeam/status/1718346358950711807) for digital forensics and incident response engagements.



(https://twitter.com/SI_FalconTeam/status/1718346358950711807)

Implant activity after hackers exploit CVE-2023-20198

source: Secuinfra Falcon Team (https://twitter.com/SI_FalconTeam/status/1718346358950711807)

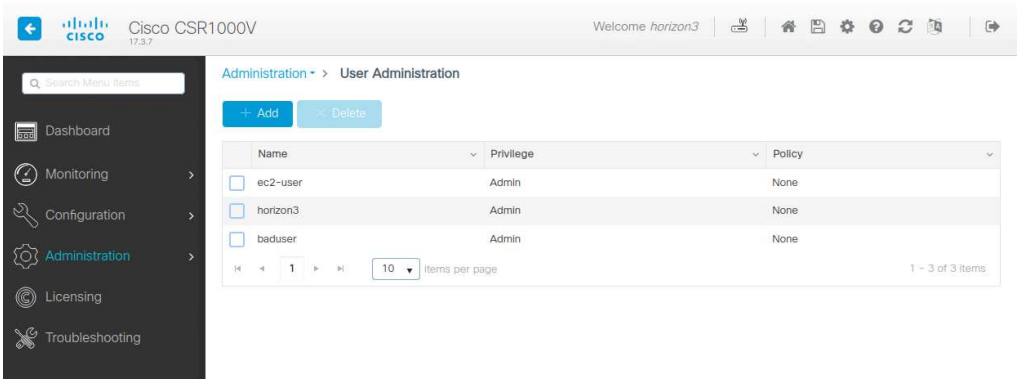
Horizon3.ai explains that an attacker can encode an HTTP request to the Web Services Management Agent (WMSA) service in *iosd* - a powerful binary in Cisco's IOS XE that can generate the configuration file for OpenResty (an Nginx-based server with support Lua scripting) used by the *webui* service vulnerable to CVE-2023-20198.

> "The crux of this vulnerability is in the first line of this request `POST /%2577ebui_wsma_HTTP`. This clever encoding of `webui_wsma_http` bypasses the Nginx matches discussed in the previous

post (https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-theory-crafting/) and allows us to reach the WMSA service in `iosd` " - Horizon3.ai

The WSMA allows executing commands through SOAP requests, including ones that give access to the configuration feature that enables creating a user with full privileges on the system.

Testing their exploit code, the researchers were able to create a new user with administrative permissions (level 15 privileges) visible in the device's management interface.



CVE-2023-20198 exploit to create full-privilege user on Cisco IOS XE
source: Horizon3.ai

The researchers note that from this point an attacker has full control over the device and could write malicious implants to disk without needing to exploit another vulnerability.

Cisco IOS XE backdoors come alive

LeakIX (https://leakix.net/), an intelligence platform for exposed online services, confirmed that the exploit that Secuinfra also observed could successfully hijack Cisco IOS XE devices.

In addition, LeakIX's Cisco IOS XE honeypots were awoken by the threat actors, allowing researchers to see commands executed on devices.

(https://twitter.com/leak_ix/status/1718323987623633035)
Attacker sends commands for reconnaissance purposes
source: LeakIX

In a PCAP file of the session shared with BleepingComputer, we can see the attackers execute the following commands:

```
show ip interface brief
show ip dns view
show ip name-servers
```

These are all commands that serve reconnaissance purposes, to collect information that would lead to the discovery of high-value targets

Cisco patches more IOS XE versions

Cisco has updated its security bulletin for CVE-2023-20198 (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z?

emailclick=CNSemail) on October 30, announcing updates for IOS XE that address the vulnerability.

At the moment version 17.3 of the software is the only one still affected by the security issue, as a new release is yet to become available. The company has also addressed the issue in Software Maintenance Updates (SMUs).

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

The new software releases are available from the company's Software Download Center (https://software.cisco.com/download/home).

Thousands of devices likely still hacked

Threat actors started exploiting CVE-2023-20198 when it was a zero-day before Cisco disclosed it on October 16.

Ten days after that, the Censys platform for threat hunting found on October 25 around 28,000 Cisco IOS XE hosts showing signs of compromise (https://censys.com/cisco-ios-xe-ten-days-later/) spread all over the world.

According to Censys' findings, many of the hacked devices are at major telecommunications and internet providers offering their services country-wide.

Initial estimates after Cisco disclosed that the vulnerability was being exploited in the wild counted around 10,000 that were running a malicious implant.

By the end of the week, internet scans showed that the implant was present on about 60,000 Cisco IOS XE devices exposed on the public web.

The number dropped suddenly shortly after, as many of the hacked devices became invisible when the threat actor altered the malicious code to check for an Authorization header before responding.

Researchers at cybersecurity company Fox-IT came up with a scanning method adjusted to the change that revealed close to 38,000 compromised Cisco IOS XE hosts on October 23.

Related Articles:

Adobe fixes Acrobat Reader zero-day with public PoC exploit (https://www.bleepingcomputer.com/news/security/adobe-fixes-acrobat-reader-zero-day-with-public-poc-exploit/)

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/)

Palo Alto Networks warns of firewall hijack bugs with public exploit (https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-firewall-hijack-bugs-with-public-exploit/)