CYBER THREAT INTELLIGENCE ANALYSIS

THREAT INTELLIGENCE ASSESSMENT ON CVE-2023-20198

DOCUMENT PREPARED BY ELLEN HALLAM
SENIOR THREAT INTELLIGENCE ANALYST

CREATED: 17TH OCTOBER 2023

OFFICIAL – SENSITIVE
CONFIDENTIAL

CVE-2023-20198 CISCO IOS XE SOFTWARE VULNERABILITY

1.1 SUMMARY:

CVE-2023-20198 is a critical vulnerability in the Web UI feature of CISCO IOS XE Software that has been actively exploited by unknown attackers. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access, which gives the attacker full control over the router. The vulnerability is triggered when the web UI feature is exposed to the internet or untrusted networks. The web UI feature is enabled through the Ip http server or Ip http secure-server commands.

Severity:

CVSS score
10

1.2 OBSERVATION:

Through the vulnerability, hackers can create an account on the affected device and gain full control of it. The vulnerability was found during the resolution of multiple Cisco Technical Assistance Centre support cases where customers were hacked. The first situation was discovered on 28th September. Following an investigation, Cisco researchers said it found activity related to the bug dating back to 18th September.
The attackers also used another vulnerability, CVE-2021-1435, to install an implant on the compromised devices. CVE-2021-1435 is a command injection vulnerability in the web UI of Cisco IOS XE Software that was patched by Cisco in March 2021. However, Cisco Talos observed that some devices that were fully patched against CVE-2021-1435 were still infected by the implant. The implant allows the attackers to execute arbitrary commands as root and communicate with a command-and-control server.

1.3 ANALYST ASSESSMENT:

The vulnerability carries the highest possible severity CVSS score of 10, as it can grant an attacker full administrator privileges, allowing them to effectively take full control of the affected router and allowing possible subsequent authorised activity.

It is assessed as *highly likely* that the same threat actor has been attacking this vulnerability. This is because both attacks appeared close together, with the September activity leading to the October activity. It is *likely* the first cluster was the actor's initial attempt at testing their code, while the October activity was *likely* the actor expanding their operation to include establishing persistent access via deployment of the implant.

© Bytes Software Services 2023 www.bytes.co.uk

1.4 ISSUE CORRECTION:

Cisco has not released a software patch, or workaround, for CVE-2023-20198 , but has provided some recommendations to narrow the attack vector until a patch is available. These include:

1. Disabling the web UI feature if it is not needed.
2. Applying access control lists (ACLs) to restrict access to the web UI feature.
3. Using firewall rules to block access to the web UI feature from untrusted sources.
4. Monitoring network logs for any suspicious activity.
5. As always, administrators need detailed information on their systems in cases like this where there is no current available patch.
6. Users of products with the software should be on the lookout for 'unexplained or newly created users on devices as evidence of potentially malicious activity relating to this threat.'

Caveat:

This is based on current, limited knowledge, which should be further investigated and checked, before being applied to your systems.

1.5 SOURCES:

1. Cisco: Hackers targeting zero-day found in internet-exposed routers (therecord.media)
2. CVE-2023-20198 : Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Softwa (cvedetails.com)
3. Cisco Releases Security Advisory for IOS XE Software Web UI | CISA

Annex 1:

The Probability Yardstick

To quantify language, we use the Probability Yardstick, from the Professional Head of Intelligence Assessment. It is a tool used by the UK Government to standardise the way we describe probability and has been used to ensure consistency across the different thematic areas and threats when providing assessments on how *likely* something is to occur. The yardstick is included for clarity.

Professional Head of Intelligence Assessment

Probability Yardstick

Probability range	Judgement terms	Fraction range
> 0 - ≤ ≈5%	***Remote chance***	> 0 - ≤ ≈1/20
≈10% - ≈20%	***Highly unlikely***	≈1/10 - ≈1/5
≈25% - ≈35%	***Unlikely***	≈1/4 - ≈1/3
≈40% - < 50%	***Realistic possibility***	≈2/5 - < 1/2
≈55% - ≈75%	***Likely*** or ***Probably***	≈5/9 - ≈3/4
≈80% - ≈90%	***Highly likely***	≈4/5 - ≈9/10
≥ ≈95% - < 100%	***Almost certain***	≥ ≈19/20 - < 1

≈ approximately ≥ is more than or equal to ≤ is less than or equal to > is more than < is less than

© Bytes Software Services 2023 www.bytes.co.uk

Source Evaluation:

We also assess our sources using the below matrix, but rarely disclose our source, to protect the integrity of the source. We assess sources on how reliable they are, how they accessed the intelligence, and we then decide if this intelligence can be shared. The table shown to the illustrates this.

Source Evaluation	Intelligence Evaluation	Handling Conditions
1 - Reliable	A - Known directly to the source	P – Lawful sharing permitted
	B - Known indirectly to the source but corroborated	
2 - Untested	C - Known indirectly to the source	C - Lawful sharing permitted with conditions
	D - Not known	
3 – Not reliable	E - Suspected to be false	

Confidence Levels:

High Confidence	High confidence generally indicates judgements based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and still carries a risk of being wrong.
Moderate Confidence	Moderate confidence generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence
Low Confidence	Low confidence generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed

© Bytes Software Services 2023
www.bytes.co.uk