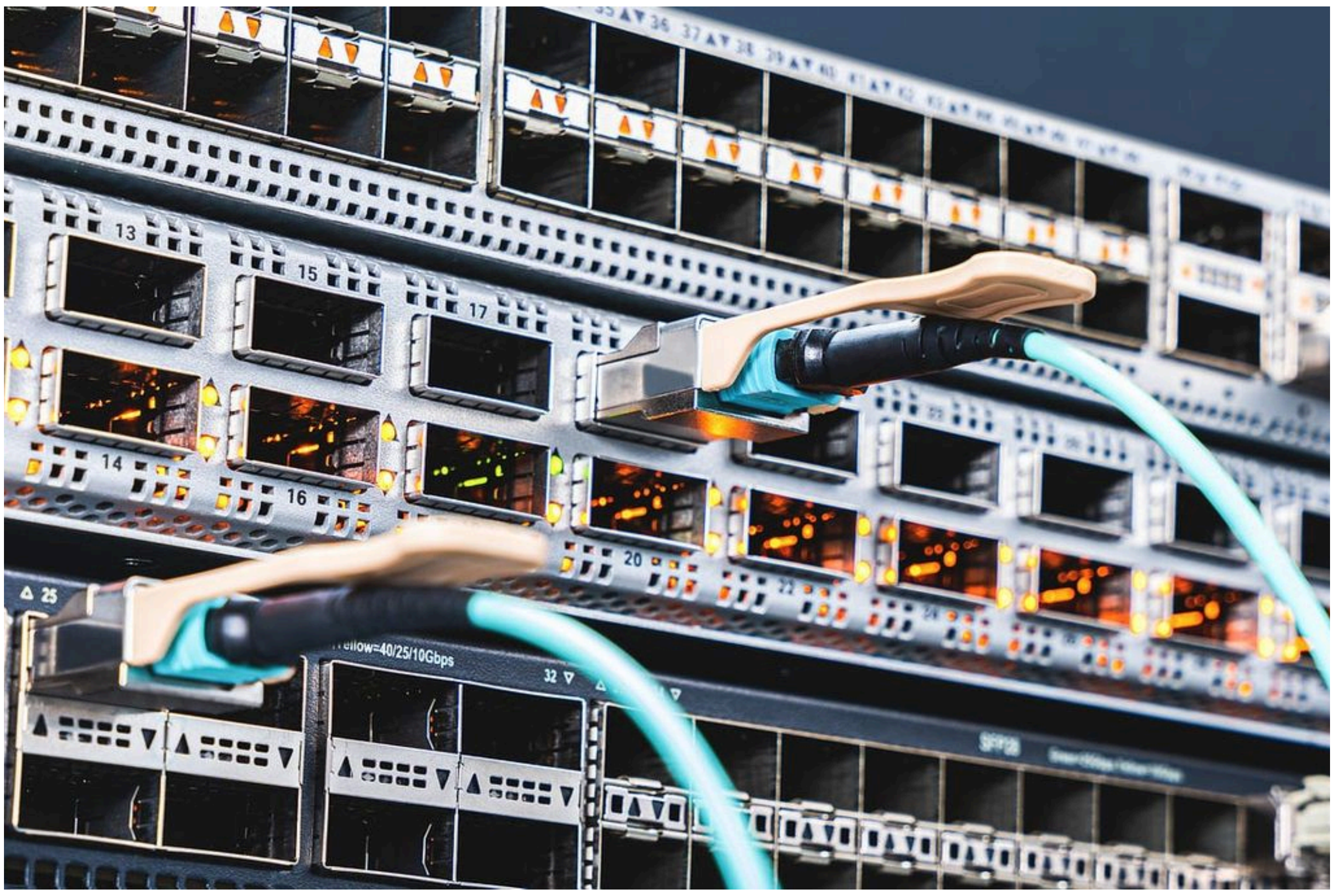
CISCO — CYBERSECURITY — NEWS

Incident response exercises urged after mass Cisco device exploitation

Cisco says patch pending October 22 for what transpires to have been two discrete zero days...

THE STACK

October 20, 2023 . 1:40 PM — 3 min read



Updated October 20, 18:12 with news of a pending fix from Cisco.

Organisations should consider triggering incident response exercises after mass exploitation of Cisco devices (with over 40,000 compromised).

Security experts at after Cisco on October 16 disclosed a CVSS 10-rated authentication bypass, CVE-2023-20198, affecting Cisco IOS XE.

The vulnerability has been mass-exploited to place malicious implants on switches and routers. (Organisations can fire out a specific HTTP POST request, which returns a certain 18-character hexadecimal string if a box has been popped.)

As Censys researchers noted tartly: “The last few weeks have seen their fair share of potential sky-crumbling advisories: The Exim vulnerability, which amounted to much of nothing, and the HTTP/2 “Rapid Reset” attack, which was only a problem for the top internet providers running bleeding-edge web technologies in heavily proxied environments. But this time, Apollo, I think we have a problem...”

Cisco says fix due October 22

Cisco IOS XE exploitation

By October 18 it was seeing 41,983 infected hosts. A day later 5,400 Cisco XE devices had either removed their web interface from the internet, been taken offline, or had their configurations reset (well done you) Censys data showed. (The current underlying implant being seen does not survive a reboot.) The number on infected devices remains a significant problem.

Threat intelligence firm Greynoise said that some devices had already been put into malicious service by attackers. Given Cisco IOS devices are also used internally in many organizations and are equally susceptible, attackers “after gaining initial access on a low-privileged endpoint” will likely be probing for vulnerable Cisco devices internally, where it is just as likely the web admin UI will be enabled, its researchers added.

Rapid7 said it had seen attackers doing the following

"The first malicious activity performed on the system post-exploitation was associated with the `admin` account. The following is an excerpt from this log file:

```
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
```

The threat actor created the local account `cisco_support` using the command `username cisco_support privilege 15 algorithm-type sha256 secret *` under user context `admin`. The threat actor then authenticated to the system using this newly created `cisco_support` account and began running several commands, including the following:

```
show running-config
show voice register global
show dial-peer voice summary
show platform
show flow monitor
show platform
show platform software iox-service
show iox-service
dir bootflash:
dir flash:
clear logging
no username cisco_support
no username cisco_tac_admin
no username cisco_sys_manager
```

"Upon completion of these commands, the threat actor deleted the account `cisco_support`. The accounts `cisco_tac_admin` and `cisco_sys_manager` were also deleted, but Rapid7 did not observe account creation commands associated with these accounts within available logs.The threat actor also executed the `clear logging` command to clear system logging and cover their tracks. Rapid7 identified logging for the second exploitation on October 12, 2023, but could not review logs for the first intrusion because the logs had been cleared."

Whilst reviewing Cisco estates/patch management, organisations should be aware that multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) that are also being exploited in the wild and which were reported this week. CVE-2023-4966 (CVSS 9.4) has a patch available. To be vulnerable, appliances must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.

Orange Cyberdefense's CERT team has shared a script to check for Cisco IOS XE exploitation here. Cisco emphasises that the recommendation it has provided in its security advisory to disable the HTTP server feature on internet-facing devices is "consistent with not only best practices but also guidance the U.S. government has provided in the past on mitigating risk from internet-exposed management interfaces."

See also: Top 10 misconfigurations: NSA checklist for CISOs flags Active Directory Certificate Services and other common issues

Related

CISCO

Cisco is still hard-coding passwords into its products

JASPER HAMILL

October 25, 2024

CISCO

Cisco celebrates "second strongest year" ever, cuts 7% of its workforce

JASPER HAMILL

August 15, 2024

CISCO

Critical Cisco vulnerability CVE-2024-20419 lets unauthenticated attackers change admin passwords

JASPER HAMILL

July 18, 2024

CISO

CISCO names former Palo Alto Networks CTO as new CISO in key region

FRANCESCA DEAN

June 11, 2024

Latest

CYBERSECURITY

Sophos attackers breached intelligence agency, wrote code to survive firmware updates

EDWARD TARGETT

November 1, 2024

CLOUD

Amazon ramps up AWS CapEx, admits capacity constraints

THE STACK

November 1, 2024

MICROSOFT

Microsoft warns of $1.5 billion OpenAI loss as it "turns away" GPU business

JASPER HAMILL

October 31, 2024

LLMS

Are hallucinating GenAI models careless or just plain ignorant? Google researchers found out

JASPER HAMILL

October 31, 2024

THE STACK

Sign up