

Hiveforce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Cisco IOS XR Flaws Enable Privilege Elevation and DoS Attacks

Date of Publication

March 15, 2024

Admiralty Code

A1

TA Number

TA2024104










Summary

First Discovered: March 2024

Affected Product: Cisco IOS XR software

Impact: Three high-severity vulnerabilities have been discovered in the Cisco IOS XR software, posing risks of denial-of-service (DoS) attacks and elevation of privilege. These vulnerabilities are tracked as CVE-2024-20320, CVE-2024-20318, and CVE-2024-20327.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-20320	Cisco IOS XR Software SSH Privilege Escalation Vulnerability	Cisco IOS XR Software			
CVE-2024-20318	Cisco IOS XR Software Denial of Service Vulnerability	Cisco IOS XR Software			
CVE-2024-20327	Cisco IOS XR Software for Routers PPPoE Services Denial of Service Vulnerability	Cisco IOS XR Software			

Vulnerability Details

#1

The Cisco IOS XR software is impacted by three high-severity vulnerabilities, specifically CVE-2024-20320, CVE-2024-20318, and CVE-2024-20327. These vulnerabilities have the potential to facilitate elevation of privilege and denial-of-service (DoS) attacks.

#2

A CVE-2024-20320 vulnerability in the SSH client feature of Cisco IOS XR Software makes it possible for a local, authorised attacker to escalate privileges on a compromised device. The SSH client CLI command's inadequate parameter validation is the cause of this vulnerability. By submitting a crafted command, an attacker with low-privileged access can take advantage of this and potentially elevate their privileges to root on the device.

#3

A DoS scenario can be created by an unauthenticated attacker by triggering the line card network processor to reset due to a vulnerability tracked as CVE-2024-20318. This vulnerability arises from improper handling of some Ethernet frames received on line cards that have the Layer 2 services option enabled. If the attack is successful, traffic over the supported interfaces can be stopped since the attacker can reset the network processor of the ingress interface. A DOS issue would arise from the line card repeatedly reset.

#4

The PPP over Ethernet (PPPoE) termination feature's inadequate validation of user-supplied information is the cause of vulnerability CVE-2024-20327. By providing the device with carefully crafted input, a remote attacker on the local network can launch a DoS attack.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20320	Cisco IOS XR Software: 7.3.2 - 7.10, 8000 Series Routers, IOS XRd Control Plane, IOS XRd vRouter, NCS 540 Series Routers, NCS 5700 Series Routers	cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*	CWE-266
CVE-2024-20318	Cisco IOS XR Software: 7.8 - 7.10 ASR 9000 Routers, ASR 9902 Routers ASR 9903 Routers, IOS XRd vRouters, IOS XRv 9000 Routers	cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*	CWE-20
CVE-2024-20327	Cisco IOS XR: 7.8 - 7.11, Cisco ASR 9000 Series Aggregation Services Routers: All versions	cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*	CWE-20

Recommendations



Apply Patch: Install the security patch provided by Cisco to address the CVE-2024-20320, CVE-2024-20318, and CVE-2024-20327 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.



Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	TA0040 Impact
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1498 Network Denial of Service
T1059 Command and Scripting Interpreter	T1059.008 Network Device CLI		

Patch Details

Update Routers to IOS XR version 7.11.1 or later

Link: <https://www.cisco.com/c/en/us/support/routers/index.html>

References

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ssh-privesc-eWDMKew3>

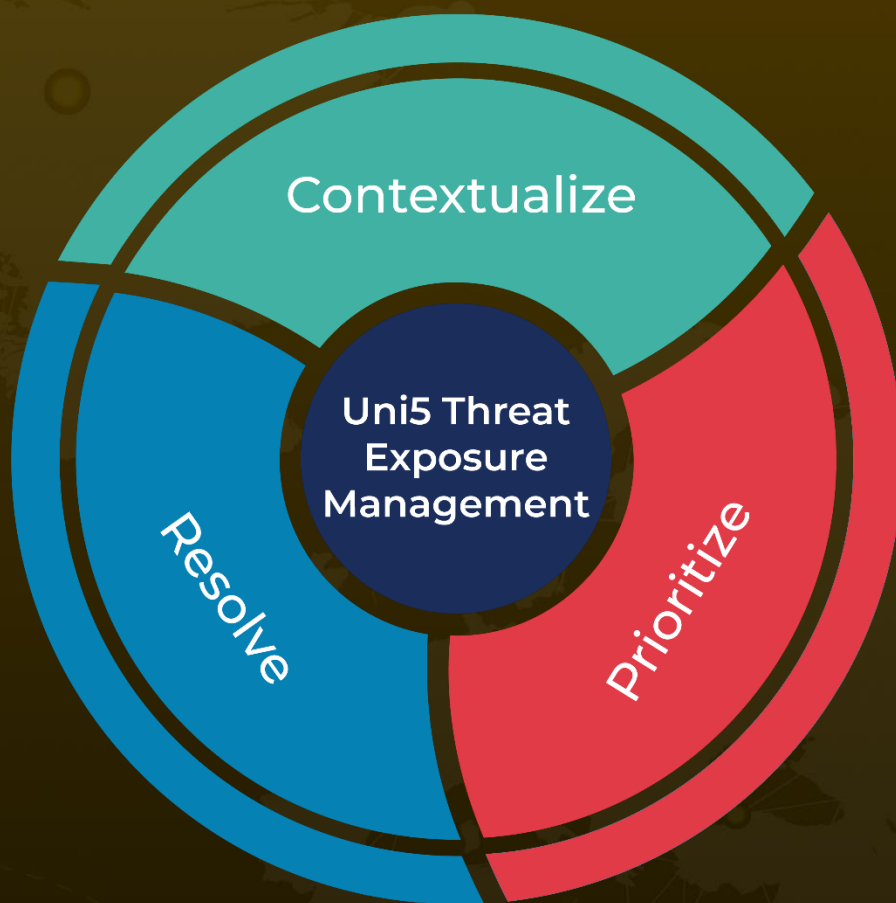
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrl2vpn-jesrU3fc>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pppma-JKWFgneW>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

March 15, 2024 • 5:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com