Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco IMC Flaw Enables Attackers to Escalate Privileges to Root

Date of Publication	Admiralty Code	TA Number
April 18, 2024	A1	TA2024153

Summary

Discovered: April 2024
Affected Products: Cisco Integrated Management Controller (IMC)
Impact: Cisco has addressed a high-severity vulnerability, identified as CVE-2024-20295, in the Command Line Interface (CLI) of the Cisco Integrated Management Controller (IMC). This vulnerability could potentially allow attackers to escalate privileges to root.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-20295	Cisco Integrated Management Controller CLI Command Injection Vulnerability	Integrated Management Controller (IMC)	✗	✗	✓

Vulnerability Details

#1 The vulnerability CVE-2024-20295 in the Cisco Integrated Management Controller (IMC) CLI is indeed concerning, as it could allow a local, authorized attacker to escalate privileges to root and potentially execute command injection attacks on the underlying operating system. Given that the attacker must have read-only or higher privileges on the affected device to exploit this vulnerability.

#2 CVE-2024-20295 poses a significant risk as it allows a local user to execute arbitrary commands on the target system. This flaw occurs due to improper input validation in the command-line interface of the application. A local user can exploit this vulnerability by passing specially crafted data to the application, thereby executing arbitrary operating system commands on the target system. If successfully exploited, this vulnerability can lead to the complete compromise of the vulnerable system.

#3 The vulnerability impacts various Cisco products running a vulnerable version of Cisco IMC in their default configurations. These include the 5000 Series Enterprise Network Compute Systems, Catalyst 8300 Series Edge uCPE, UCS C-Series Rack Servers, and UCS E-Series Servers.

#4 Cisco appliances based on a preconfigured version of a Cisco UCS C-Series Server expose access to the Cisco IMC CLI, they are also affected by the vulnerability. It's important for administrators to ensure that all affected devices are patched or updated to mitigate the risk of exploitation. Proof-of-concept exploit code for the vulnerability is already circulating, but fortunately, threat actors have not yet begun to exploit it in attacks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20295	Cisco Integrated Management Controller: 3.2.6 - 4.12 Enterprise NFV Infrastructure Software: 3.12 - 3.13 Cisco 5000 Series Enterprise Network Compute System: All versions Catalyst 8300 Series Edge Universal CPE: All versions UCS C-Series Rack Servers in standalone mode: All versions UCS E-Series Servers: All versions	cpe:2.3:a:cisco:integrated_management_controller:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Patch: Install the security patch provided by Cisco to address the CVE-2024-20295 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

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.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1202 Indirect Command Execution	T1059 Command and Scripting Interpreter
T1059.008 Network Device CLI	T1068 Exploitation for Privilege Escalation		

Patch Details

Apply the software patches provided by Cisco to address the vulnerability and ensure the security of their systems.

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

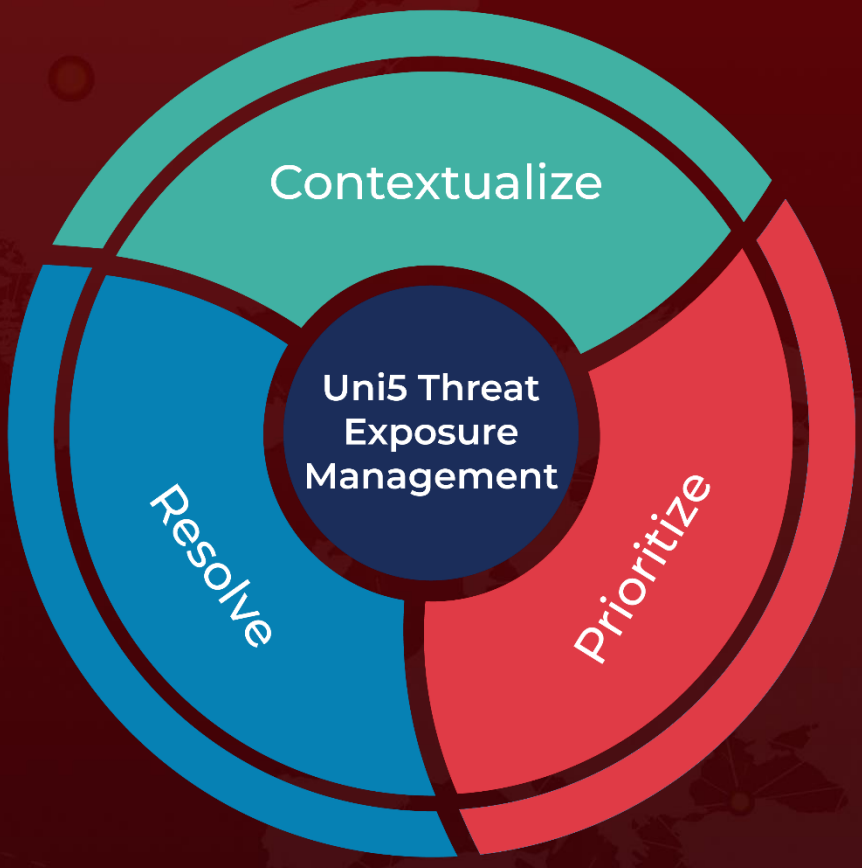
References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

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

April 18, 2024 • 6:15 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com