Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Multiple Command Injection Vulnerabilities Found in Cisco EPNM, ISE, and Prime Infrastructure

Date of Publication	Admiralty Code	TA Number
April 07, 2023	A1	TA2023173

Summary

First Seen: April 5, 2023
Affected Product: Cisco Evolved Programmable Network Manager (EPNM), Cisco Identity Services Engine (ISE), Cisco Prime Infrastructure
Impact: An attacker with authenticated, local access can exploit these vulnerabilities to escape the restricted shell and gain root privileges on the operating system.

⚙ CVEs

CVE	NAME	PATCH	CISA KEV
CVE-2023-20121	Cisco EPNM, Cisco ISE, and Cisco Prime Infrastructure Command Injection Vulnerability	✓	✗
CVE-2023-20122	Cisco ISE Command Injection Vulnerability	✓	✗

Vulnerability Details

Cisco has announced the discovery of multiple vulnerabilities in their Evolved Programmable Network Manager (EPNM), Identity Services Engine (ISE), and Prime Infrastructure software. These vulnerabilities are caused by an error in the validation of the parameters sent to a certain command within the restricted shell of these products. These vulnerabilities could allow an authenticated, local attacker to escape the restricted shell and gain root privileges on the underlying operating system. The vulnerabilities are not dependent on one another, and the exploitation of one is not required to exploit another. Cisco has released software updates to address these vulnerabilities, and there are no known workarounds.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20121	Evolved Programmable Network (EPN) Manager: 7.0 Cisco Identity Services Engine (ISE): 3.2 Cisco Prime Infrastructure: 3.9 - 3.10	cpe:2.3:a:cisco_systems:evolved_programmable_network_manager:*:*:*:*:*:*:*:*	CWE-77
CVE-2023-20122	Cisco Identity Services Engine (ISE): 3.2	cpe:2.3:a:cisco_systems:cisco_identity_services_engine:3.2:*:*:*:*:*:*:*	CWE-77

Recommendations

To mitigate these vulnerabilities, Cisco regularly releases patches and updates to its software, and it is crucial for organizations utilizing Cisco products to stay current with these releases and promptly apply any necessary updates to ensure the security of their systems.

Besides keeping software up to date, organizations can take proactive steps to decrease their vulnerability to potential attacks. These measures may include implementing network segmentation, restricting access to sensitive systems, and regularly monitoring network activity for any signs of suspicious or malevolent behavior.

Uni5 Users: This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0040 Impact	T1059 Command and Scripting Interpreter	T1587 Develop Capabilities	T1068 Exploitation for Privilege Escalation
T1587.004 Exploits	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	

Patch Link

https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

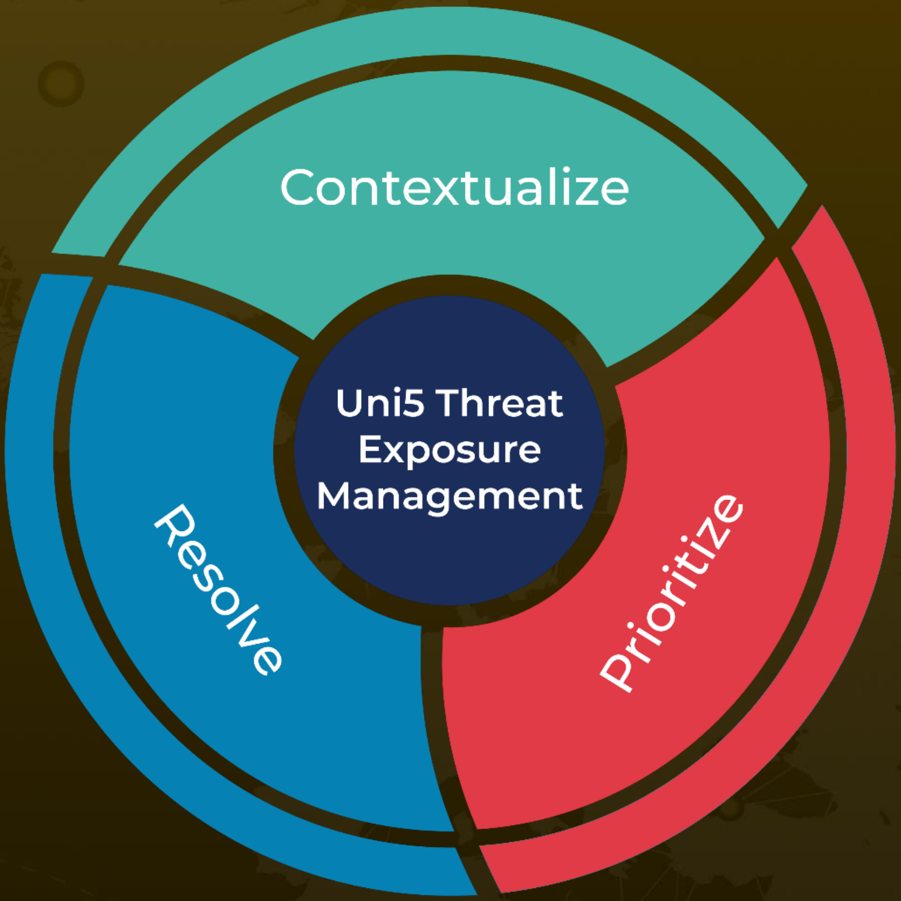
References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk

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 07, 2023 • 01:30 AM

More at www.hivepro.com