

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Unpatched Cisco ISE Devices at Risk of Root Compromise

Date of Publication

September 5, 2024

Admiralty Code

A1

TA Number

TA2024341




Summary

First Seen: September 4, 2024

Affected Product: Cisco Identity Services Engine

Impact: CVE-2024-20469 is a command injection vulnerability in Cisco Identity Services Engine (ISE), allowing authenticated local attackers with admin privileges to execute arbitrary commands and escalate to root. This flaw stems from insufficient input validation in certain CLI commands. Proof-of-concept exploit code is available, raising the risk of exploitation. Cisco has released patches in ISE versions 3.2P7 and 3.3P4 to address the issue.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20469	Cisco Identity Services Engine Command Injection Vulnerability	Cisco Identity Services Engine			

Vulnerability Details

#1

CVE-2024-20469 is a command injection vulnerability found in the Cisco Identity Services Engine (ISE). This flaw allows an authenticated local attacker with administrator privileges to inject commands into the system's CLI (Command Line Interface). Exploiting this vulnerability could enable the attacker to elevate their privileges to root, gaining full control of the underlying operating system.

#2

The root cause of CVE-2024-20469 lies in the insufficient validation of user-supplied input within certain CLI commands. Attackers can craft malicious commands, which may be executed due to a lack of proper input sanitization. This relatively straightforward attack requires local access and administrative privileges.

#3

The exploitation of CVE-2024-20469 can have severe consequences for organizations relying on Cisco ISE for network management and security, allowing attackers to manipulate system settings, access sensitive information, and potentially execute further attacks within the network.

#4

The availability of publicly disclosed proof-of-concept (PoC) exploit code increases the risk of exploitation. Cisco has released patches to address the issue in ISE versions 3.2P7 (September 2024) and 3.3P4 (expected to be released in October 2024). Organizations are strongly encouraged to apply these patches promptly, as there are no workarounds available.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20469	Cisco Identity Services Engine (ISE) versions: 3.2 and 3.3	cpe:2.3:a:cisco:identity_services_engine:3.2.0:*:*:*:*:*	CWE-78

Recommendations



Apply Security Patches Immediately: Cisco has released patches for Cisco Identity Services Engine (ISE) in versions 3.2P7 (September 2024) and 3.3P4 (October 2024), which contain fixes for this vulnerability. Ensure that all instances of Cisco ISE in your environment are updated promptly to minimize exposure to potential exploitation.



Limit Access to Admin Privileges: Restrict administrator access to only those who need it. Since the vulnerability requires admin-level access to be exploited, limiting the number of users with this access can reduce potential attack vectors.



Monitor for Unauthorized Access: Implement robust logging and monitoring for unusual command-line activity, especially by users with admin privileges. Set up alerts for unauthorized or suspicious access attempts and privilege escalation within Cisco ISE.



Use Role-Based Access Control (RBAC): Enforce role-based access control to minimize the scope of potential damage from compromised accounts. Ensure that users are given only the permissions necessary to perform their tasks.



Conduct Regular Security Audits: Perform regular vulnerability assessments and audits of network security settings. Regularly review and test access controls, especially in systems handling sensitive information like Cisco ISE.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>TA0004</u> Privilege Escalation	<u>T1588.005</u> Exploits
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1588</u> Obtain Capabilities	<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities
<u>T1548</u> Abuse Elevation Control Mechanism	<u>T1078</u> Valid Accounts	<u>T1059.008</u> Network Device CLI	

Patch Details

Upgrade Cisco Identity Services Engine (ISE) versions to 3.2P7 (available in September 2024) and 3.3P4 (to be released in October 2024).

Link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-6kn9tSxm>

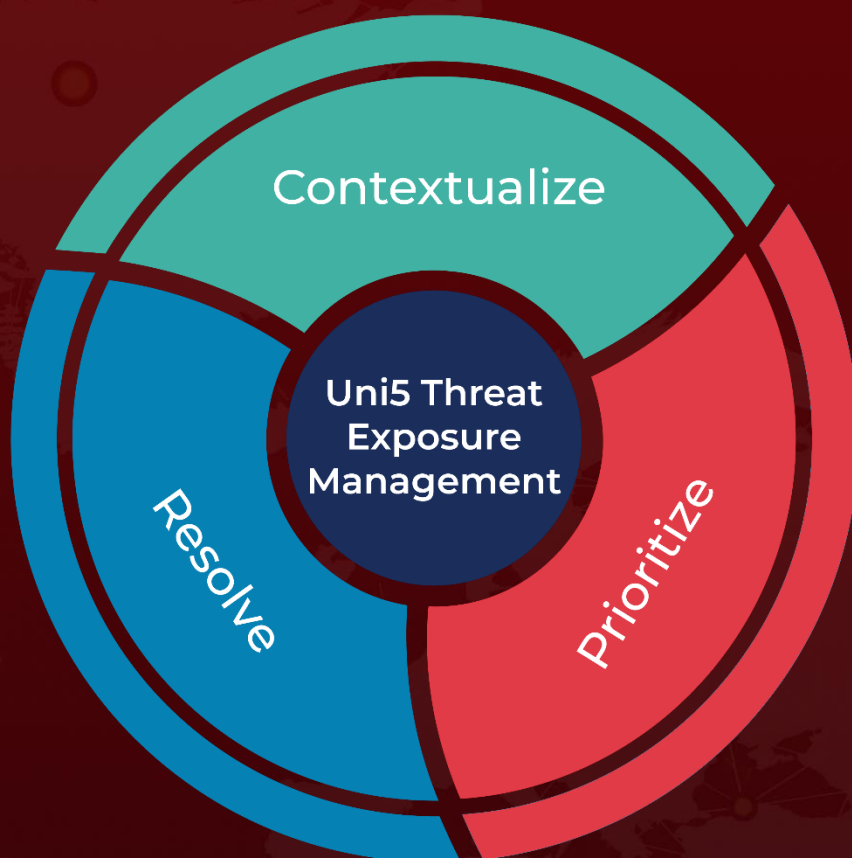
References

<https://www.blackhatethicalhacking.com/news/cisco-patches-critical-ise-command-injection-vulnerability-with-public-exploit-code>

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

September 5, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com