Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Smart Licensing Utility Vulnerabilities Exploited in the Wild

Date of Publication	Last Updated Date	Admiralty Code	TA Number
September 11, 2024	April 3, 2025	A1	TA2024350

Summary

First Seen: September 4, 2024
Affected Products: Cisco Smart Licensing Utility
Affected Platform: Windows and Linux
Impact: Cisco has issued security updates to address two critical vulnerabilities, CVE-2024-20439 and CVE-2024-20440, in its Smart Licensing Utility. These vulnerabilities could allow unauthenticated remote attackers to elevate privileges or access sensitive information. Though independent, these vulnerabilities are being actively exploited by attackers and can be chained together to further enhance the attack's effectiveness. Cisco has urged users to update to version 2.3.0 immediately, as no workarounds exist.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-20439	Cisco Smart Licensing Utility Static Credential Vulnerability	Cisco Smart Licensing Utility	✗	✓	✓
CVE-2024-20440	Cisco Smart Licensing Utility Information Disclosure Vulnerability	Cisco Smart Licensing Utility	✗	✗	✓

Vulnerability Details

#1 Cisco has issued security updates for two critical vulnerabilities, CVE-2024-20439 and CVE-2024-20440, in its Smart Licensing Utility (SLU). These vulnerabilities, both rated with a CVSS score of 9.8, pose significant risks by allowing unauthenticated remote attackers to either elevate privileges or access sensitive information. While these flaws are independent exploiting one does not require exploiting the other they are actively being targeted in the wild.

#2 CVE-2024-20439 is a critical vulnerability caused by an undocumented static user credential for an administrative account embedded in the SLU application. Attackers can exploit this flaw to log into affected systems using these static credentials, gaining administrative privileges over the API. This vulnerability is particularly dangerous as it provides attackers with direct access to manage licensing services. Cisco has confirmed active exploitation of this flaw, with attackers leveraging it as an entry point to compromise vulnerable systems.

#3 CVE-2024-20440 is an information disclosure vulnerability stemming from excessive verbosity in debug log files. Attackers can send specially crafted HTTP requests to retrieve these log files, which may contain sensitive data such as API credentials. These credentials can then be used to access the API and further compromise the system. This vulnerability is being exploited alongside CVE-2024-20439, forming a potent attack chain where initial access via static credentials is followed by sensitive data extraction.

#4 Both vulnerabilities are exploitable only if the Cisco Smart Licensing Utility is actively running on the system, limiting exposure somewhat. However, confirmed exploitation activity has been observed since March 2025, with attackers scanning for exposed SLU instances online. Cisco has released patches addressing these vulnerabilities but emphasized that no workarounds exist. Users must upgrade to SLU version 2.3.0 or later to mitigate these risks effectively.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20439	Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0	cpe:2.3:a:cisco:smart_license_utility:*:*:*:*:*:*:*:*	CWE-912
CVE-2024-20440	Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0	cpe:2.3:a:cisco:smart_license_utility:*:*:*:*:*:*:*:*	CWE-532

Recommendations

Update: Upgrade to Cisco Smart Licensing Utility version 2.3.0 or later, as these versions are not affected by CVE-2024-20439 and CVE-2024-20440. Cisco has confirmed that no workarounds exist, making updates essential.

Disable Unnecessary Services: Ensure the CSLU application is not running unless required, as these vulnerabilities are only exploitable when the utility is actively running.

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

Monitor for Exploitation: Regularly review system logs for suspicious activity, such as unauthorized login attempts or unusual API requests, which could indicate exploitation of these vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0010 Exfiltration	TA0002 Execution	TA0004 Privilege Escalation
TA0006 Credential Access	T1588 Obtain Capabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation
T1005 Data from Local System	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter	T1078.001 Default Accounts	T1078 Valid Accounts	T1552.001 Credentials In Files

Patch Details

Users are urged to update to the latest software version 2.3.0 to address the vulnerabilities CVE-2024-20439 and CVE-2024-20440. Prompt application of these updates is crucial to mitigate the risks associated with these security flaws.

Link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

References

https://www.cisa.gov/news-events/alerts/2024/09/10/cisco-releases-security-updates-cisco-smart-licensing-utility

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

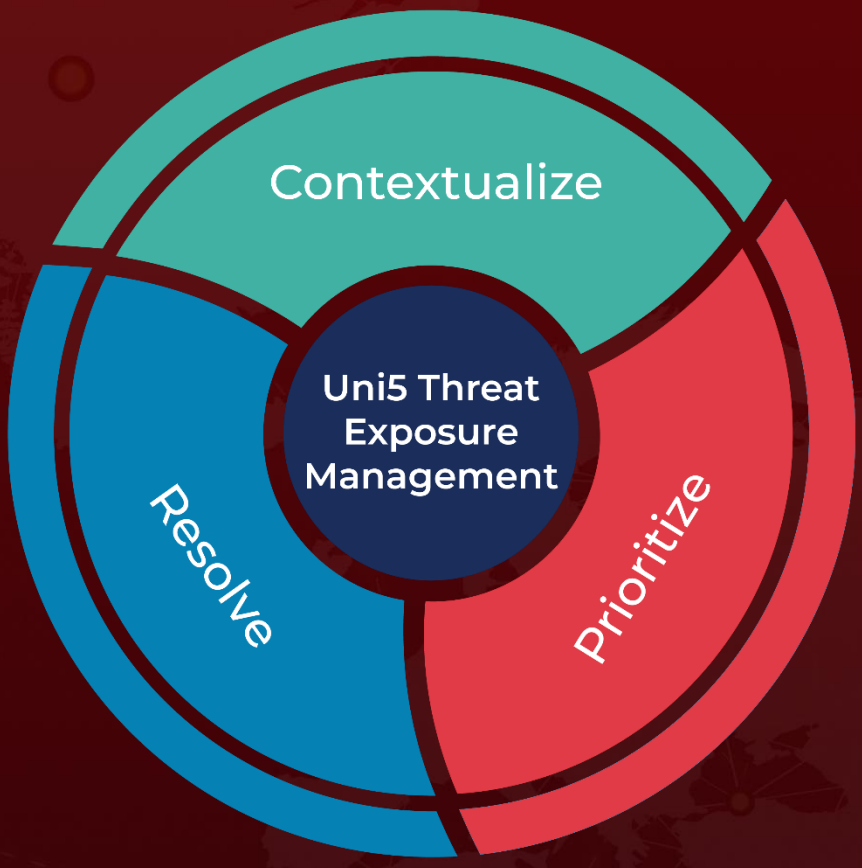
https://isc.sans.edu/diary/rss/31782

https://starkeblog.com/cve-wednesday/cisco/2024/09/20/cve-wednesday-cve-2024-20439.html

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 11, 2024 • 7:15 AM

More at www.hivepro.com