Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Smart Licensing Utility Flaws Enable Remote Privilege Escalation

Date of Publication	Admiralty Code	TA Number
September 11, 2024	A1	TA2024350

Summary

First Seen: September 4, 2024
Affected Products: Cisco Smart Licensing Utility
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 enable unauthenticated remote attackers to elevate privileges or access sensitive information. All systems running a vulnerable version of the Cisco Smart Licensing Utility are affected, regardless of their software configuration.

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. These flaws could allow unauthenticated remote attackers to either elevate privileges or access sensitive information. They affect any system running a vulnerable version of the utility, regardless of configuration, and are independent of each other—exploiting one does not depend on the other.

#2 CVE-2024-20439 allows unauthenticated remote attackers to log in to an affected system using a static administrative credential. This issue stems from an undocumented static user credential for an admin account, enabling attackers to gain administrative access through the Cisco Smart Licensing Utility API.

#3 The CVE-2024-20440 vulnerability allows a remote attacker to access sensitive information. By sending a specially crafted HTTP request, an attacker can obtain log files that contain sensitive information, including credentials. These credentials can then be used to access the API, posing a significant security risk.

#4 These vulnerabilities are only exploitable if the Cisco Smart Licensing Utility is actively running on the system. While this limits the exposure, users should ensure the utility is not running unnecessarily to minimize the risk of exploitation.

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: Cisco has released software updates to address the vulnerabilities CVE-2024-20439 and CVE-2024-20440. Users are strongly encouraged to apply these updates immediately to protect their systems from potential exploitation.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	TA0006 Credential Access
TA0010 Exfiltration	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation
T1059 Command and Scripting Interpreter	T1078 Valid Accounts	T1078.001 Default Accounts	T1552 Unsecured Credentials
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

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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

September 11, 2024 • 7:15 AM

More at www.hivepro.com