BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

September 11, 2024

Cisco Smart Licensing Utility Vulnerability

SUMMARY

Cisco recently addressed two critical vulnerabilities (CVE-2024-20439 and CVE-2024-20440) in the Cisco Smart Licensing Utility (CSLU), removing a backdoor administrative account and fixing an information disclosure flaw. These vulnerabilities could allow remote attackers the ability to gain unauthorized administrative access or retrieve sensitive data. Users are advised to update to the latest version to prevent exploitation.

RISK SCORE

CVE-ID	CVSSv3 Score
CVE-2024-20439	9.8
CVE-2024-20440	9.8

VULNERABILITY DETAILS

CSLU is a Windows-based tool designed to manage licenses and associated products locally, without the need to connect to Cisco's cloud-based Smart Software Manager.

The first flaw, CVE-2024-20439, involved a backdoor account that allowed unauthorized attackers to log in with administrative privileges using static, hardcoded credentials, through the API of the Cisco Smart Licensing Utility application. This vulnerability was particularly dangerous and allowed attackers to gain full access to systems remotely without authentication.

The second flaw, CVE-2024-20440, involved the exposure of sensitive log files containing API credentials, accessible through crafted HTTP requests. This vulnerability impacted only certain versions of the CSLU and posed a significant risk by leaking sensitive data that could be used in further attacks.

AFFECTED PRODUCTS

- Cisco Smart License Utility 2.0.0, 2.1.0, and 2.2.0

REMEDIATION

- Update to Cisco Smart License Utility 2.3.0 or later.

REFERENCES

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
- https://thehackernews.com/2024/09/cisco-fixes-two-critical-flaws-in-smart.html
- https://www.bleepingcomputer.com/news/security/cisco-warns-of-backdoor-admin-account-in-smart-licensing-utility/