مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Cisco Smart Licensing Utility

Tracking #:432316225

Date:05-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to collect sensitive information.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in Cisco's Smart Licensing Utility (CSLU), which could allow unauthenticated, remote attackers to collect sensitive information or gain administrative access to systems running the software. Cisco has released updates to address these vulnerabilities, but there are no workarounds available.

- **CVE-2024-20439**- CVSS Base Score: 9.8,Critical- Cisco Smart Licensing Utility Static Credential Vulnerability
- **CVE-2024-204340**- CVSS Base Score: 9.8,Critical- Cisco Smart Licensing Utility Information Disclosure Vulnerability

Affected Products and Fixed releases:

Cisco Smart License Utility Release	First Fixed Release
2.0.0	Migrate to a fixed release.
2.1.0	Migrate to a fixed release.
2.2.0	Migrate to a fixed release.
2.3.0	Not vulnerable.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Cisco's Smart Licensing Utility to the fixed version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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