IMPORTANT CYBERSECURITY NEWS: CRITICAL CISCO SMART LICENSING UTILITY FLAWS NOW EXPLOITED IN ATTACKS

Vairav Cyber Security News Report

Date: March 21st, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Recent reports indicate that attackers are actively exploiting two critical vulnerabilities in Cisco's Smart Licensing Utility (CSLU), identified as CVE-2024-20439 and CVE-2024-20440. These flaws allow unauthenticated, remote attackers to gain administrative access and extract sensitive information from affected systems. The exploitation of these vulnerabilities poses significant risks, including unauthorized system control and data breaches.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Attackers are leveraging a static credential vulnerability (CVE-2024-20439) in the CSLU, which permits unauthorized administrative access. Additionally, an information disclosure flaw (CVE-2024-20440) allows attackers to retrieve sensitive data from log files.

- **CVE-2024-20439**: A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential. This vulnerability affects Cisco Smart Licensing Utility Release versions 2.0.0, 2.1.0, and 2.2.0. It is strongly recommended that users upgrade to respective fixed releases for these versions.

- **CVE-2024-20440**: A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to access sensitive information. This vulnerability affects Cisco Smart Licensing Utility Release versions 2.0.0, 2.1.0, and 2.2.0. It is strongly recommended that users upgrade to respective fixed releases for these versions.

Identification: The SANS Internet Storm Center reported observing exploitation attempts against these vulnerabilities, initially disclosed by Cisco in September 2024.

Affected Entities/Industries: Organizations utilizing Cisco's Smart Licensing Utility across various industries are at risk.

Potential Impact: Risks include unauthorized system access, data breaches, operational disruptions, and potential financial losses.

Exploitation Methods: Attackers exploit hardcoded administrative credentials to gain unauthorized access and extract sensitive information from log files.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply the patches provided by Cisco to address CVE-2024-20439 and CVE-2024-20440.
- Ensure that the CSLU application is not running unnecessarily, as it is not designed to run in the background by default.

Security Best Practices

- Regularly update and patch all software and applications.
- Monitor network traffic for unusual activities.
- Implement strong access controls and authentication mechanisms.

For Advanced Security Teams

- Conduct threat hunting exercises focusing on unauthorized access patterns related to CSLU.
- Develop and deploy intrusion detection system (IDS) signatures to identify exploitation attempts of these vulnerabilities.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/critical-cisco-smart-licensing-utility-flaws-now-exploited-in-attacks/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com