مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

LPE vulnerability in Sophos Intercept X

Tracking #:432316358

Date:03-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption.

TECHNICAL DETAILS:

Sophos has addressed a local privilege escalation vulnerability in the Device Encryption component of Sophos Intercept X for Windows, which allowed for arbitrary file writing. This fix is crucial for maintaining the security integrity of affected systems.

Key Details:
CVE ID: CVE-2024-8885 |8.8,High|
Affected Versions: The vulnerability impacts Sophos Intercept X for Windows with Central Device Encryption versions 2024.2.0 and older.
Fix Release: The remediation was included in the update to Device Encryption version 2024.2.1.6,

- FTS: 2024.2.3.9.2 and newer
- LTS: 2024.1.0.45 and newer

RECOMMENDATIONS:

- Users of Sophos Intercept X to verify their current versions and apply the necessary updates to safeguard against this vulnerability.

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://www.sophos.com/en-us/security-advisories/sophos-sa-20241002-cde-lpe