مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in Sophos Intercept X

Tracking #:432317562

Date:04-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities in Sophos Intercept X that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Sophos has addressed three distinct local privilege escalation vulnerabilities affecting various components of Sophos Intercept X for Windows, including the updater, installer, and Device Encryption module. These vulnerabilities could allow a local attacker to gain SYSTEM-level privileges under certain conditions.

High-Severity Vulnerabilities:

- **CVE-2024-13972**: A vulnerability in the updater's registry permissions may allow a local user to elevate privileges during a product upgrade.
- **CVE-2025-7433:** A flaw in the Device Encryption component enables local privilege escalation via arbitrary code execution.
- **CVE-2025-7472:** A local user can gain SYSTEM-level privileges by exploiting the Intercept X for Windows installer when executed as SYSTEM.

Affected products:

- **CVE-2024-13972:**
  - Sophos Intercept X for Windows prior to Core Agent version 2024.3.2
- **CVE-2025-7433:**
  - Sophos Intercept X for Windows Central Device Encryption prior to version 2025.1
- **CVE-2025-7472**
  - Sophos Intercept X for Windows Installer prior to version 1.22

Remediation:

- **CVE-2024-13972:**
  - Sophos Intercept X for Windows Core Agent 2024.3.2
  - Sophos Intercept X for Windows FTS 2024.3.2.23.2
  - Sophos Intercept X for Windows LTS 2025.0.1.1.2
  - Sophos Intercept X for Windows Server FTS 2024.3.2.23.2
  - Sophos Intercept X for Windows Server LTS 2025.0.1.1.2

- **CVE-2025-7433:**
  - Device Encryption 2025.1 on July 1, 2025
  - Sophos Intercept X for Windows FTS 2024.3.2.23.2
  - Sophos Intercept X for Windows LTS 2025.0.1.1.2

- **CVE-2025-7472**
  - Sophos Intercept X for Windows Installer 1.22

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the updates released by Sophos.

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-20250717-cix-lpe