Date Posted: 2025/07/25

[Vulnerability Alert] Two Significant Security Vulnerabilities in Sophos Intercept X for Windows

- Subject: [Vulnerability Alert] Two Significant Security Vulnerabilities in Sophos Intercept X for Windows
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000013
  - Sophos recently released a security advisory regarding Intercept X for Windows, indicating that the product has two significant security vulnerabilities and has provided patched versions. Users are urged to check their systems and apply relevant updates as soon as possible.
  - [CVE-2024-13972, CVSS: 8.8] This vulnerability exists in the update program of Sophos Intercept X for Windows and is related to registry permission settings. Attackers may gain system-level privileges through local users during product upgrades.
  - [CVE-2025-7433, CVSS: 8.8] A local privilege escalation vulnerability exists in the device encryption component of Sophos Intercept X for Windows, which allows attackers to execute arbitrary code.
- Affected Platforms:
  - Sophos Intercept X for Windows versions prior to 2024.3.2 (excluding)
  - Sophos Intercept X for Windows Central Device Encryption versions prior to 2025.1 (excluding)
- Recommended Action:
  - Apply patches according to the solutions released on the official website: https://www.sophos.com/en-us/security-advisories/sophos-sa-20250717-cix-lpe
- References:
  - https://www.twcert.org.tw/tw/cp-169-10276-19d7a-1.html

Computer and Communications Center
Network Systems Group

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250725_01

Last update: **2025/07/25 15:38**