Date Posted: 2025/08/04

[Vulnerability Alert] Sophos Firewall System Has 3 Significant Security Vulnerabilities

- Subject: [Vulnerability Alert] Sophos Firewall System Has 3 Significant Security Vulnerabilities
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000021
  - Sophos has released a security advisory for its firewall products, indicating that they have three significant security vulnerabilities, and has provided patched versions. Users are urged to check their systems and apply relevant updates as soon as possible.
  - [CVE-2025-6704, CVSS: 9.8] A remote arbitrary file write vulnerability exists in the Secure PDF eXchange (SPX) feature. If specific configurations of SPX are enabled and the firewall is in high-availability (HA) mode, it may lead to pre-authenticated remote code execution.
  - [CVE-2025-7624, CVSS: 9.8] A SQL injection vulnerability exists in the Legacy (transparent) SMTP proxy. If email quarantine policies are enabled and the system is upgraded from a version prior to 21.0 GA to the current version, it may lead to remote code execution.
  - [CVE-2025-7382, CVSS: 8.8] A command injection vulnerability exists in WebAdmin. If the administrator enables OTP authentication, it may allow an adjacent attacker to achieve pre-authenticated code execution on the high-availability (HA) auxiliary device.
- Affected Platforms:
  - Sophos Firewall v21.5 GA (inclusive) and earlier versions
- Recommended Action:
  - Apply patches according to the solutions released on the official website: https://www.sophos.com/en-us/security-advisories/sophos-sa-20250721-sfos-rce
- References:
  - https://www.twcert.org.tw/tw/cp-169-10280-e36be-1.html

Computer and Communications Center
Network Systems Group