مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Sophos Firewall

Tracking #:432317513

Date:22-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Sophos has disclosed multiple critical vulnerabilities in its Firewall. The vulnerabilities allow attackers to achieve remote or pre-auth code execution, arbitrary file writing, SQL and more.

TECHNICAL DETAILS:

Sophos has issued a security advisory addressing several critical and high-severity vulnerabilities that have been fixed in its Firewall. Exploitation of these vulnerabilities may allow attackers to achieve remote or pre-auth code execution, arbitrary file writing, SQL and command injection, and DNS manipulation across various Sophos components including SPX, SMTP proxy, WebAdmin, and Up2Date, under specific configurations and conditions.

Vulnerability Details:

CVE ID	Description	Severity
CVE-2025-6704	An arbitrary file writing vulnerability in the Secure PDF eXchange (SPX) feature can lead to pre-auth remote code execution, if a specific configuration of SPX is enabled in combination with the firewall running in High Availability (HA) mode.	CRITICAL
CVE-2025-7624	An SQL injection vulnerability in the legacy (transparent) SMTP proxy can lead to remote code execution, if a quarantining policy is active for Email and SFOS was upgraded from a version older than 21.0 GA.	CRITICAL
CVE-2025-7382	A command injection vulnerability in WebAdmin can lead to adjacent attackers achieving pre-auth code execution on High Availability (HA) auxiliary devices, if OTP authentication for the admin user is enabled.	HIGH

CVE ID	Description	Severity
CVE-2024-13974	A business logic vulnerability in the Up2Date component can lead to attackers controlling the firewall's DNS environment to achieve remote code execution.	HIGH
CVE-2024-13973	A post-auth SQL injection vulnerability in WebAdmin can potentially lead to administrators achieving arbitrary code execution.	MEDIUM

Affected product(s) and version(s):

- **CVE-2024-13974, CVE-2024-13973:**
  - Sophos Firewall v21.0 GA (21.0.0) and older
- **CVE-2025-6704, CVE-2025-7624, CVE-2025-7382:**
  - Sophos Firewall v21.5 GA (21.5.0) and older

Remediation:

- **CVE-2025-6704:**
  - Hotfixes for the following supported versions published on:
    - June 24 2025 for 19.0 MR2 (19.0.2.472), 20.0 MR2 (20.0.2.378), 20.0 MR3 (20.0.3.427), 21.0 GA (21.0.0.169), 21.0 MR1-2 (21.0.1.277), 21.5 GA (21.5.0.171)
    - July 1 2025 for 21.0 MR1 (21.0.1.237), 21.0 MR1-1 (21.0.1.272)
  - Fix first included in v21.0 MR2 and newer

- **CVE-2025-7624:**
  - Hotfixes for the following supported versions published on:
    - July 15 2025 for 19.0 MR2 (19.0.2.472), 20.0 MR2 (20.0.2.378), 20.0 MR3 (20.0.3.427), 21.0 GA (21.0.0.169), 21.0 MR1 (21.0.1.237), 21.0 MR1-1 (21.0.1.272), 21.0 MR1-2 (21.0.1.277), 21.5 GA (21.5.0.171)
  - Fix first included in v21.0 MR2 and newer

- **CVE-2025-7382:**
  - Hotfixes for the following supported versions published on:
    - June 30 2025 for 19.0 MR2 (19.0.2.472), 20.0 MR2 (20.0.2.378), 20.0 MR3 (20.0.3.427), 21.0 GA (21.0.0.169), 21.0 MR1-2 (21.0.1.277), 21.5 GA (21.5.0.171)
    - July 2 2025 for 21.0 MR1 (21.0.1.237), 21.0 MR1-1 (21.0.1.272)
  - Fix first included in v21.0 MR2 and newer

- **CVE-2024-13974:**
  - Hotfixes for the following supported versions published on:
    - January 6 2025 for 19.0 MR2 (19.0.2.472)
    - January 7 2025 for 20.0 MR2 (20.0.2.378), 20.0 MR3 (20.0.3.427), 21.0 GA (21.0.0.169)
  - Fix first included in v21.0 MR1 and newer

- **CVE-2024-13973:**
  - Fix first included in v21.0 MR1 and newer
  - Users of older versions of Sophos Firewall are required to upgrade to receive the latest protections, and this fix

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest 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-20250721-sfos-rce