مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Critical Vulnerabilities Sophos Firewall

Tracking #:432316653

Date:20-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Sophos has released security updates to address multiple vulnerabilities in its firewall product.

TECHNICAL DETAILS:

Sophos has issued security updates to address three significant vulnerabilities affecting its Sophos Firewall product. These vulnerabilities, identified as CVE-2024-12727, CVE-2024-12728, and CVE-2024-12729, could potentially allow remote attackers to compromise systems and gain unauthorized access.

Vulnerabilities Details:

1. **CVE-2024-12727: Pre-auth SQL Injection (CVSS 9.8 Critical)**
    - A pre-authentication SQL injection vulnerability exists within the email protection feature of Sophos Firewall. Exploiting this flaw could allow attackers to access the reporting database, potentially enabling remote code execution if specific conditions are met (Secure PDF eXchange (SPX) enabled and High Availability (HA) mode configured).
    - **Impact:** Remote code execution, unauthorized access to the reporting database.
2. **CVE-2024-12728: Insecure SSH Passphrase (CVSS 9.8 Critical)**
    - This vulnerability stems from the reuse of a suggested non-random SSH login passphrase after the HA establishment process. If SSH is enabled, this flaw could expose privileged system accounts.
    - **Impact:** Privilege escalation, potential unauthorized access.
3. **CVE-2024-12729: Post-auth Code Injection (CVSS 8.8 High)**
    - This post-authentication vulnerability allows authenticated users to execute arbitrary code through the User Portal.
    - **Impact:** Unauthorized code execution by authenticated users.

Affected Versions:

Sophos Firewall v21.0 GA (21.0.0) and older versions

Remediation:

- CVE-2024-12727:
    - Hotfixes for the following versions published on:
        - Dec 17 2024 for v21 GA, v20 GA, v20 MR1, v20 MR2, v20 MR3, v19.5 MR3, v19.5 MR4, v19.0 MR2
    - Fix included in v21 MR1 and newer
- CVE-2024-12728:
    - Hotfixes for the following versions published on:
        - Nov 26 2024 for v21 GA, v20 GA, v20 MR1, v19.5 GA, v19.5 MR1, v19.5 MR2, v19.5 MR3, v19.5 MR4, v19.0 MR2
        - Nov 27 2024 for v20 MR2
    - Fix included in v20 MR3, v21 MR1 and newer
- CVE-2024-12729:
    - Hotfixes for the following versions published on:
        - Dec 04 2024 for v21 GA, v20 GA, v20 MR1, v20 MR2
        - Dec 05 2024 for v19.5 GA, v19.5 MR1, v19.5 MR2, v19.5 MR3, v19.5 MR4,

v19.0 MR2, v19.0 MR3
- Dec 10 2024 for v20 MR3
- Fix included in v21 MR1 and newer

Workarounds:
For CVE-2024-12728:
- Restrict SSH access to the dedicated HA link
- Reconfigure HA using a long, random custom passphrase

For CVE-2024-12729:
- Ensure User Portal and Webadmin are not exposed to WAN
- Disable WAN access to User Portal and Webadmin
- Use VPN or Sophos Central for remote management

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-20241219-sfos-rce