Patch Now – Three Sophos Firewall Vulnerabilities

Overview

Sophos has addressed three significant vulnerabilities in its Sophos Firewall product, which could allow threat actors to exploit systems through remote code execution (RCE), SQL injection, and privileged SSH access.

Vulnerability Breakdown

- CVE-2024-12727 - Pre-authentication SQL injection vulnerability in the email protection feature, potentially leading to RCE. This issue impacts approximately 0.05% of devices with specific configurations of Secure PDF eXchange (SPX) enabled in High Availability (HA) mode.
- CVE-2024-12728 - A non-random SSH login passphrase for HA cluster initialization remains active after setup, exposing devices to unauthorized SSH access. This flaw affects approximately 0.5% of systems where SSH is enabled.
- CVE-2024-12729 - Authenticated users can exploit a code injection vulnerability in the User Portal, allowing for remote execution of arbitrary code and privilege escalation.

Affected Products

- Sophos Firewall version 21.0 GA and earlier.

Sophos has released hotfixes and permanent fixes for the vulnerabilities. Although these vulnerabilities have not been exploited, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Update your Sophos Firewall to version 21 MR1 or newer. See Sophos' advisory for patch guidance.
    - For specific hotfix release information, refer to Sophos' knowledge base (KBA-000010084).
- **Mitigation**
    - For CVE-2024-12728 - Restrict SSH access to dedicated HA links, reconfigure HA setups with strong, random passphrases, and disable SSH over WAN interfaces.
    - For CVE-2024-12729 - Disable WAN access to User Portal and Webadmin interfaces and use VPN or Sophos Central for remote management.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers may exploit vulnerable Sophos Firewall configurations to gain access.
- Valid Accounts (T1078) – Exploitation of predictable SSH passphrases (CVE-2024-12728) or compromised credentials (CVE-2024-12729).

Execution

- Command and Scripting Interpreter (T1059) – Use of the code injection vulnerability (CVE-2024-12729) to execute arbitrary commands.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) – Using the code injection vulnerability to escalate privileges on compromised systems.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The targeted industries for these vulnerabilities is broad. Any organization using Sophos firewalls could be impacted:

- Government
- Education
- Energy and Utilities
- Healthcare
- Finance
- Manufacturing
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the

- expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Resolved Multiple Vulnerabilities in Sophos Firewall (CVE-2024-12727, CVE-2024-12728, CVE-2024-12729) | Sophos

Sophos Firewall: Verify if the hotfixes for CVEs 2024-12727, 2024-12728, and 2024-12729 have been applied

Device access - Sophos Firewall