CERT-EU

Security Advisory 2024-120

Critical Vulnerabilities in Sophos Firewall

2024-12-20 — v1.0

TLP:CLEAR

History:

- *20/12/2024 — v1.0 – Initial publication*

Summary

On December 19, 2024, Sophos has released critical security updates addressing multiple vulnerabilities in its firewall products. These flaws could allow attackers to escalate privileges or execute arbitrary code [1,2].

Technical Details

The vulnerability **CVE-2024-12727**, with a CVSS score of 9.8, is a pre-auth SQL injection vulnerability in the email protection feature allowing access to the reporting database of Sophos Firewall. If exploited, this vulnerability could lead to remote code execution on the affected device. This vulnerability affects devices with a specific configuration where Secure PDF eXchange (SPX) is enabled in combination with the firewall running in High Availability (HA) mode.

The vulnerability **CVE-2024-12728**, with a CVSS score of 9.8, is due to the suggested and non-random SSH login passphrase for High Availability (HA) cluster initialisation remaining active after the HA establishment process is completed. If exploited, this vulnerability could expose a privileged system account on the Sophos Firewall if SSH is enabled.

The vulnerability **CVE-2024-12729**, with a CVSS score of 8.8, is a post-auth code injection vulnerability in the User Portal allowing authenticated users to gain remote code execution.

Affected Products

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

Recommendations

It is recommended applying the hotfixes or the workarounds (described below) provided by the vendor.

Workarounds

CVE-2024-12728

To mitigate the issue of the SSH passphrase (used during deployment of HA ports) remaining active, customers can ensure that:

- SSH access is restricted to only the dedicated HA link that is physically separate, and/or
- HA is reconfigured using a sufficiently long and random custom passphrase

It is also recommended disabling WAN access via SSH by following device access best practices[3] and instead use VPN and/or Sophos Central for remote access and management.

CVE-2024-12729

It is recommended ensuring that the User Portal and Webadmin console are not exposed to the Internet.

References

[1] https://www.sophos.com/en-us/security-advisories/sophos-sa-20241219-sfos-rce

[2] https://cybersecuritynews.com/sophos-firewall-vulnerabilities/

[3] https://docs.sophos.com/nsg/sophos-firewall/latest/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html