Security Advisory 2022-065

RCE Vulnerability in Sophos Firewall

September 26, 2022 — v1.0

TLP:WHITE

History:

- *26/09/2022 — v1.0 – Initial publication*

Summary

On September 23, 2022, **Sophos** warned about a critical code injection security vulnerability in the company's Firewall product that is being exploited in the wild. They observed the vulnerability being used to target a small set of specific organisations, primarily in the South Asia region [1].

Technical Details

Tracked as **CVE-2022-3236**, the flaw was found in the User Portal and Webadmin of Sophos Firewall, allowing attackers to execute code (RCE) [2, 3].

Affected Products

Sophos Firewall v19.0 MR1 (19.0.1) and older.

Recommendations

The company says it has released hotfixes for **Sophos Firewall** versions affected by this security bug (v19.0 MR1 (19.0.1) and older) that will roll out automatically to all instances since automatic updates are enabled by default.

No action is required for ***Sophos Firewall*** *customers with the* ***"Allow automatic installation of hotfixes"*** *feature enabled on remediated versions. Enabled is the default setting* [1].

In order to receive the CVE-2022-3236 patch an upgrade to a supported version of Sophos Firewall must be done.

Sophos also provided detailed info on enabling the automatic hotfix installation feature[1] and checking if the hotfix was successfully installed[2].

[1] https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/Firmware/index.html#updating-ha-devices

[2] https://support.sophos.com/support/s/article/KB-000043853

Workarounds

Sophos provided a workaround for customers who cannot immediately patch the vulnerable software. This will require them to ensure that the firewall's **User Portal** and **Webadmin** are not exposed to WAN access.

"*Disable WAN access to the **User Portal** and **Webadmin** by following device access best practices*[3] *and instead use VPN and/or Sophos Central (preferred) for remote access and management*," the company added [2].

References

[1] https://www.bleepingcomputer.com/news/security/sophos-warns-of-new-firewall-rce-bug-exploited-in-attacks/

[2] https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce

[2] https://cve.report/CVE-2022-3236

[3] https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html