Security Advisory 2022-021

Critical RCE Vulnerability in Sophos Firewalls

March 31, 2022 — v1.1

TLP:WHITE

History:

- *28/03/2022 — v1.0 – Initial publication*
- *31/03/2022 — v1.1 – Update about active exploitation*

Summary

On 25/03/2022, Sophos has fixed a critical vulnerability (CVE-2022-1040) [2] in Sophos firewall product, which allows remote code execution. This vulnerability enables an unauthenticated attacker to gain control over the targeted system. This vulnerability has a score of 9.8 out of 10 [1].

[Update] : This vulnerability is currently under **active exploitation** in the wild [3].

CERT-EU strongly recommends to patch this vulnerability **as soon as possible**.

Technical Details

An authentication bypass vulnerability allowing remote code execution was discovered in the User Portal and Webadmin of Sophos Firewall and responsibly disclosed to Sophos. The vulnerability was reported to the security firm by an unnamed security researcher via its bug bounty program.

Affected Products

Sophos Firewall v18.5 MR3 (18.5.3) and older.

Recommendations and Workarounds

Sophos released hotfixes that should, by default, reach most instances automatically. *"There is no action required for Sophos Firewall customers with the"Allow automatic installation of hotfixes" feature enabled. Enabled is the default setting."* [4].

Below is the list of products that have their hotfixes ready to be installed:

- Hotfixes for v17.0 MR10 EAL4+, v17.5 MR16 and MR17, v18.0 MR5(-1) and MR6, v18.5 MR1 and MR2, v18.5 MR3, and v19.0 EAP have been published.

- Hotfixes for unsupported EOL versions v17.5 MR12 through MR15, v18.0 MR3 and MR4, and v18.5 GA have been published.
- Fix included in v19.0 GA and v18.5 MR4 (18.5.4)
- Users of older versions of Sophos Firewall are required to upgrade to receive the latest protections and fix.

In order to check if the issue has been fixed, Sophos has published an article on their website [5].

As a general workaround, it is recommended to protect from external attackers by ensuring that the User Portal and Webadmin are not exposed to the Internet.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-1040

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1040

[3] https://thehackernews.com/2022/03/critical-sophos-firewall-rce.html

[4] https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

[5] https://support.sophos.com/support/s/article/KB-000043853?language=en_US