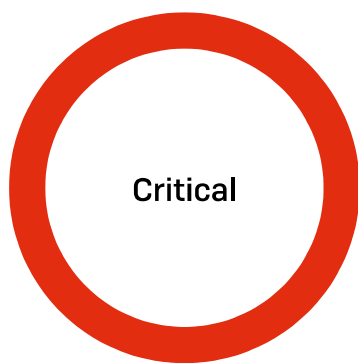




# Resolved RCE in Sophos Firewall (CVE-2022-1040)

[← Back to Security Advisories Overview \(" attr\(href\) "\)](#)

**CVE(s)**

CVE-2022-1040

**Updated:** 2022 Apr 5

**Product(s)**

Sophos Firewall

**Publication ID:** sophos-sa-20220325-sfos-rce

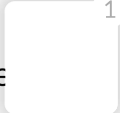
**Article Version:** 3

**First Published:** 2022 Mar 25

**Workaround:** Yes

---

## Overview

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

There is no action required for Sophos Firewall customers with the "Allow automatic installation of hotfixes" feature enabled. Enabled is the default setting.

Sophos has observed this vulnerability being used to target a small set of specific organizations primarily in the South Asia region. We have informed each of these organizations directly. Sophos will provide further details as we continue to investigate.

## Applies to the following Sophos product(s) and version(s)

Sophos Firewall v18.5 MR3 [18.5.3] and older

## Workaround

Customers can protect themselves from external attackers by ensuring their User Portal and Webadmin are not exposed to WAN.

Disable WAN access to the User Portal and Webadmin by following [device access best practices \(" attr\(href\) "\)](#) and instead use VPN and/or Sophos Central for remote access and management.

## Remediation

- Hotfixes for v17.0 MR10 EAL4+, v17.5 MR16 and MR17, v18.0 MR5(-1) and MR6, v18.5 MR1 and MR2, and v19.0 EAP published on March 23, 2022
- Hotfixes for unsupported EOL versions v17.5 MR12 through MR15, and v18.0 MR3 and MR4 published on March 23, 2022
- Hotfixes for unsupported EOL version v18.5 GA published on March 24, 2022
- Hotfixes for v18.5 MR3 published on March 24, 2022
- Hotfixes for unsupported EOL version v17.5 MR3 published on April 4, 2022
- 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 this fix

## Related information

- [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1040 \(" attr\(href\) "\)](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1040 ()
- To confirm that the hotfix has been applied to your firewall, please refer to [KB-00123 \(" attr\(href\) "\)](#).

- <https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.htm> ("attr(href)")

### Change Log:

- 2022-03-25: First Published
- 2022-03-28 22:10 UTC: Updated Overview text with additional information from Sophos investigation
- 2022-04-05: Updated hotfix release information for v17.5 MR3

## Sophos Responsible Disclosure Policy

To learn about Sophos security vulnerability disclosure policies and publications, see the [Responsible Disclosure Policy](#). ("attr(href)")

