National Cyber Security Centre

2203291524-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Remote Code Execution Vulnerability in Sophos Firewall CVE-2022-1040

2022-03-29

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

An authentication bypass vulnerability, CVE-2022-1040, allowing remote code execution has been identified in the User Portal and Webadmin of Sophos Firewalls. This vulnerability was discovered by an external researcher and reported via the Sophos bug bounty program. The vulnerability has been patched and no action is required for Sophos Firewall customers with the "Allow automatic installation of hotfixes" feature enabled. This is enabled as default.

The vulnerability has a CVSSv3 score of 9.8.

Products Affected

Sophos Firewall v18.5 MR3 (18.5.3) and older

Impact

Potential Remote Code Execution (RCE), data theft, operations disruption, ransomware, denial of service.

Recommendations

The NCSC recommends that affected organisations review the Sophos Advisory and apply the relevant patches as soon as possible.

The following remediation steps are available:

- 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
- Fix included in v19.0 GA and v18.5 MR4 (18.5.4)
- It is recommended that users of older versions of Sophos Firewall upgrade to receive the latest protections and this fix

Workaround:
Users can protect themslves 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 and instead use VPN and/or Sophos Central for remote access and management.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie