Advisory Alert

Alert Number : AAA20220329 **Date :** March 29, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sophos Firewall	**Critical**	**Remote code execution**

Description

Affected Product	Sophos Firewall
Severity	**Critical**
Affected Vulnerability	Remote code execution (CVE-2022-1040)
Description	Sophos has issued Security Updates to address a Remote code execution that exists in Firewall product. The authentication bypass vulnerability resides in the User Portal and Webadmin of the firewall. Successful exploitation of the vulnerability may allow an attacker to perform remote code execution. Sophos highly recommends to apply necessary fixes immediately to avoid issues. Hotfixes are also available for end-of-life (EOL) versions of the Sophos Firewall.
Affected Products	Sophos Firewall v18.5 MR3 (18.5.3) and older.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.