Exploited Critical Vulnerability in Sophos Firewall

29th March 2022

Ticket Number: EN250306

This advisory is sent out in part that stakeholders hold preventative management and precautions of their network.

SOPHOS

Summary

A critical vulnerability has been disclosed in Sophos Firewall. CVE-2022-1040, which has a CVSS score of 9.8, can allow an unauthenticated remote attacker to execute arbitrary code on the vulnerable system. Exploitation of this vulnerability can lead to the attacker gaining full control over the vulnerable system. This vulnerability arose due to an authentication bypass flaw. Sophos Firewall with versions 18.5.3 and older are affected. If the '*Allow automatic installations of hotfixes*' feature is enabled, entities should not do anything else apart from making sure that the product is updated to the latest version. This vulnerability is currently being exploited in the wild. In additions, Sophos also urges users of Sophos Firewall to disable WAN access to the User Portal and Webadmin interfaces. In addition, unsupported versions (17.5.12 – 17.5.15, 18.0.3 - 18.0.4 and 18.5 GA) are also being updated.

CSIRTMalta encourage everyone to make sure that Sophos Firewall is updated to the latest versions as soon as possible to mitigate any exploitations which is currently taking place in the wild.

Additional Information and References:

1. Sophos Advisory on CVE-2022-1040
2. CERT-EU's Advisory on CVE-2022-1040

CSIRTMalta Team

MINISTRY FOR HOME AFFAIRS
NATIONAL SECURITY AND LAW ENFORCEMENT