UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00259

SOPHOS CRITICAL FIREWALL BUG

DATE ISSUED: 30th March 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Sophos has released a Hot Fix for a critical bug present in their user portal and webadmin of Sophos Firewall which had the potential to allow Remote Code Execution (RCE).

BREAKDOWN

After being reported via the Sophos Bug Bounty program, Sophos have released a hotfix to remediate the vulnerability CVE-2022-1040 with a CVSS rating of 9.8 that would allow a user to bypass authentication and possibly allow an attacker to deploy arbitrary code remotely. Little detail has been released by Sophos as to the nature of the potential exploit and affect devices are the Sophos Firewall versions 18.5 MR3 and earlier. Older versions of the Firewall may require manual remediation and in some cases should be upgraded as no fix is available.

REMEDIATION STEPS

- Enable "Allow automatic installation of hotfixes" in the Sophos admin portal
  - 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)
- Users of older versions of Sophos Firewall are required to upgrade to receive the latest protections and this fix
- Workaround: Disable WAN Access to the platform entirely

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/critical-sophos-security-bug-rce-firewalls/179127/
Sophos	https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/
ZDNet	https://www.zdnet.com/article/sophos-patches-critical-remote-code-execution-vulnerability-in-firewall-defense-product/