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

CYBER GUIDANCE ISSUE 00260

SPRING4SHELL JAVA RCE ZERO-DAY

DATE ISSUED: 13th April 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

- Apply latest patches released March 31, 2022.

REFERENCES & RESOURCES

LunaSec https://www.lunasec.io/docs/blog/spring-rce-vulnerabilities/
Praetorian https://www.praetorian.com/blog/spring-core-jdk9-rce/
Threatpost https://threatpost.com/critical-rce-bug-spring-log4shell/179173/