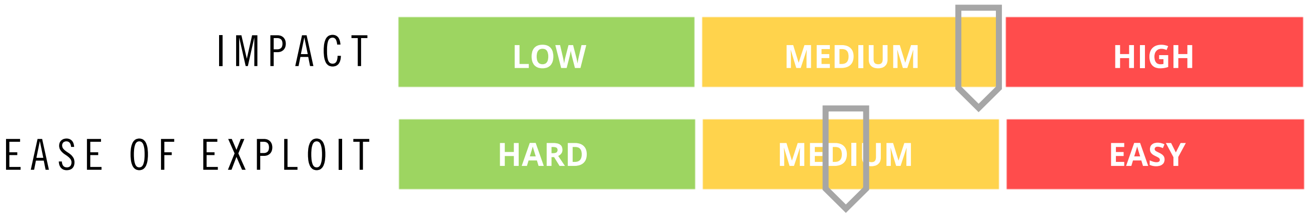
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0304

SOPHOS CRITICAL WEB APPLIANCE VULNERABILITIES

DATE ISSUED: 10th April 2023



OVERVIEW

Sophos released security updates that address several vulnerabilities in its Web Appliance. The most serious of these is a critical authenticated code execution bug. The appliance is a web security solution that enables administrators to set and enforce web access policies from a single interface.

BREAKDOWN

The Sophos Web Appliance is an enterprise solution that can function as a web proxy that provides HTTP Security at the gateway where potentially risky content is scanned for various forms of malware. The critical issue tracked as CVE-2023-1671 (CVSS score of 9.8) is a pre-auth command injection vulnerability in the warning page handler of the appliance, allowing for the execution of arbitrary code without authentication. Sophos has released Sophos Web Appliance version 4.3.10.4, which also fixes another two bugs. The first is a high-severity code execution issue in the exception wizard tracked as CVE-2022-4934 (CVSS score of 7.2) and described as a command injection vulnerability. The second is CVE-2020-36692, a medium-severity cross-site scripting (XSS) flaw in the report scheduler. An attacker could exploit the vulnerability to execute JavaScript code in the victim's browser. Sophos Web Appliance is set to reach end-of-life (EOL) status on July 20, 2023. Sophos recommends that Web Appliance customers migrate to Sophos Firewall before it reaches end-of-life (EOL) status on July 20, 2023.

REMEDIATION STEPS

- Patches for all vulnerabilities are delivered to Sophos Web Appliance users via automatic updates.
- Sophos recommends placing the appliance behind a firewall and blocking internet access.

REFERENCES & RESOURCES

Security Week	https://www.securityweek.com/sophos-patches-critical-code-execution-vulnerability-in-web-security-appliance/
Sophos	https://www.sophos.com/en-us/security-advisories/sophos-sa-20230404-swa-rce