Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Sophos Zero-day vulnerability becomes target for attackers

Date of Publication	Admiralty Code	TA Number
September 26, 2022	A1	TA2022212

Summary

A zero-day vulnerability in the User Portal and WebAdmin of Sophos Firewall has been tracked as CVE-2022-3236. This vulnerability is been used by some unknown attackers to target organizations in South Asia.

CVE Table

CVE	NAME	PATCH
CVE-2022-3236	Remote Code Execution in Sophos Firewall	✓

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**TA0001** Initial Access
T1190 Exploit Public-Facing Application			

Technical Details

#1 This code injection zero-day vulnerability, CVE-2022-3236, exists in the User Portal and Webadmin of the Sophos Firewall. An attacker can successfully exploit this vulnerability for remote code execution (RCE).

#2 Sophos published hotfixes to address this vulnerability, which have been automatically deployed to all susceptible devices because of the 'Allow automatic installation of hotfixes' functionality that is activated by default. However, hotfixes published for end-of-life Sophos Firewall versions must be manually upgraded in order to address the security issue and defend against ongoing assaults. Customers can also defend themselves from external attackers by not exposing their User Portal and Webadmin to the WAN.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-3236	Sophos Firewall: 17.0.0 - 19.0.1	cpe:2.3:h:sophos:xg_firewall:*:*:*:*:*:*:*:*	CWE-94

Patch Details

Upgrade to Sophos Firewall v18.5 MR5 (18.5.5), v19.0 MR2 (19.0.2), and v19.5 GA

References

https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 26, 2022 • 11:00 AM

More at www.hivepro.com