

CVE-2022-1040

Sophos Firewall Authentication Bypass Vulnerability

Exigent

CISA KEV since Mar 31, 2022

Actively exploited

An authentication bypass vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v18.5 MR3 and older.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Apr 21, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
sfos	≤ 18.5.3	after 18.5.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-9gcv-6rm7-vw3w

Additional guidance sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

NVD nvd.nist.gov/vuln/detail/CVE-2022-1040

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-24387

Current data evulnable.com/vulnerability-management/cve/CVE-2022-1040

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.