Sophos Firewall Authentication Bypass Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-1040
State	PUBLIC
Assigner	security-alert@sophos.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-25 12:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	An authentication bypass vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sopho

Risk And Classification

EPSS: 0.944390000 probability, percentile 0.999890000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-31; due 2022-04-21; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Sophos
Product	Firewall
Name	Sophos Firewall Authentication Bypass Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2022-1040

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sophos	Sfos	All	All	All	All

References

Reference	Source	Link	Tag
Sophos XG115w Firewall 17.0.10 MR-10 - Authentication Bypass - Hardware webapps Exploit	MISC	www.exploit-db.com	
www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce	CONFIRM	www.sophos.com	
Sophos XG115w Firewall 17.0.10 MR-10 Authentication Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	can

NVD vulnerability detail	NVD	nvd.nist.gov	can
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730411 Sophos Firewall Remote Code Execution (RCE) Vulnerability (sophos-sa-20220325-sfos-rce)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**