

CVE-2020-29574

Sophos CyberoamOS (CROS) SQL Injection Vulnerability

Exigent

CISA KEV since Feb 6, 2025

Actively exploited

Ransomware use known

An SQL injection vulnerability in the WebAdmin of Cyberoam OS through 2020-12-04 allows unauthenticated attackers to execute arbitrary SQL statements remotely.

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.047 91.7th percentile · FIRST	CISA DEADLINE Feb 27, 2025 KEV since 2025 · 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	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.047 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: The impacted product is end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue utilization of the product.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
cyberoamos	≤ 2020-12-04	after 2020-12-04	NVD

Sources

Vendor guidance github.com/advisories/GHSA-v2fr-wv49-j53x

support.sophos.com support.sophos.com/support/s/article/KBA-000007526

NVD nvd.nist.gov/vuln/detail/CVE-2020-29574

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-21936

Current data evulnable.com/vulnerability-management/cve/CVE-2020-29574

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