

CVE-2025-23006

SonicWall SMA1000 Appliances Deserialization Vulnerability

Exigent

CISA KEV since Jan 24, 2025

Actively exploited

Ransomware use known

Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands.

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.234 97.8th percentile · FIRST	CISA DEADLINE Feb 14, 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	0.234 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 mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 7 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma8200v	< 12.4.3-02854	12.4.3-02854	NVD
sma6200 firmware	< 12.4.3-02854	12.4.3-02854	NVD
sma6210 firmware	< 12.4.3-02854	12.4.3-02854	NVD
sma7200 firmware	< 12.4.3-02854	12.4.3-02854	NVD
sma7210 firmware	< 12.4.3-02854	12.4.3-02854	NVD
sra ex6000 firmware	≤ 12.4.3-02804	after 12.4.3-02804	NVD
sra ex7000 firmware	≤ 12.4.3-02804	no fixed version listed	NVD
sra ex9000 firmware	≤ 12.4.3-02804	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-57r3-2prp-v2xh

Additional guidance psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002

NVD nvd.nist.gov/vuln/detail/CVE-2025-23006

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-3070

Current data evulnable.com/vulnerability-management/cve/CVE-2025-23006

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