

CVE-2023-44221

SonicWall SMA100 Appliances OS Command Injection Vulnerability

CISA KEV since May 1, 2025

Actively exploited

Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated attacker with administrative privilege to inject arbitrary commands as a 'nobody' user, potentially leading to OS Command Injection Vulnerability.

EVRS 78_{/100} Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.762 99.54th percentile · FIRST	CISA DEADLINE May 22, 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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.762 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 2 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma 200 firmware	≤ 10.2.1.9-57sv	after 10.2.1.9-57sv	NVD
sma 210 firmware	≤ 10.2.1.9-57sv	after 10.2.1.9-57sv	NVD
sma 400 firmware	≤ 10.2.1.9-57sv	after 10.2.1.9-57sv	NVD
sma 410 firmware	≤ 10.2.1.9-57sv	after 10.2.1.9-57sv	NVD
sma 500v firmware	≤ 10.2.1.9-57sv	after 10.2.1.9-57sv	NVD
sma 200	—	no fixed version listed	NVD
sma 210	—	no fixed version listed	NVD
sma 400	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-q6mf-v98h-w783

Additional guidance psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

NVD nvd.nist.gov/vuln/detail/CVE-2023-44221

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-48580

Current data evulnable.com/vulnerability-management/cve/CVE-2023-44221

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