

CVE-2026-15409

SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability

Exigent
CISA KEV since Jul 14, 2026
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.

EVRS 85 /100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.068 94th percentile · FIRST	CISA DEADLINE Jul 17, 2026 CISA federal deadline · Overdue by 3 months
--	---	--	--

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 year
☒ EPSS	0.068 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma8200v	12.4.3-03245 12.4.3-03387 12.4.3-03434 12.5.0-02283 12.5.0-02624 12.5.0-02800	no fixed version listed	NVD
sma6210 firmware	12.4.3-03245 12.4.3-03387 12.4.3-03434 12.5.0-02283 12.5.0-02624 12.5.0-02800	no fixed version listed	NVD
sma7210 firmware	12.4.3-03245 12.4.3-03387 12.4.3-03434 12.5.0-02283 12.5.0-02624 12.5.0-02800	no fixed version listed	NVD
sma6210	—	no fixed version listed	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
sma7210	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-35rc-2vcv-r6q5	Additional guidance	psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-15409	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-44404	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-15409

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