

CVE-2019-7483

SonicWall SMA100 Directory Traversal Vulnerability

CISA KEV since Mar 28, 2022

Actively exploited

In SonicWall SMA100, an unauthenticated Directory Traversal vulnerability in the handleWAFRedirect CGI allows the user to test for the presence of a file on the server.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.040 90.5th percentile · FIRST	CISA DEADLINE Apr 18, 2022 KEV since 2022 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.040 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma 100 firmware	< 9.0.0.4	9.0.0.4	NVD
sma 100	—	no fixed version listed	NVD

Sources

Vendor guidance	psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0018	NVD	nvd.nist.gov/vuln/detail/CVE-2019-7483
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-17025
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-7483		

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