

CVE-2021-20016

SonicWall SSLVPN SMA100 SQL Injection Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x.

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.400 98.6th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.400 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 3 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma 500v	—	no fixed version listed	NVD
sma 100 firmware	≥ 10.0.0.0 < 10.2.0.5-d-29sv	10.2.0.5-d-29sv	NVD
sma 200 firmware	—	no fixed version listed	NVD
sma 210 firmware	—	no fixed version listed	NVD
sma 400 firmware	—	no fixed version listed	NVD
sma 410 firmware	—	no fixed version listed	NVD
sma 100	—	no fixed version listed	NVD
sma 200	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-c283-6775-92m9

Additional guidance psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

NVD nvd.nist.gov/vuln/detail/CVE-2021-20016

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-7479

Current data evulnable.com/vulnerability-management/cve/CVE-2021-20016

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