

CVE-2021-20028

SonicWall Secure Remote Access (SRA) SQL Injection Vulnerability

Exigent

CISA KEV since Mar 28, 2022

Actively exploited

Ransomware use known

Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier

EVRS

85/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.301

98.2nd 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.301 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:** The impacted product is end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 4 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
sma 210 firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sma 410 firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sma 500v firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sra 4600 firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sra 1600 firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sra va firmware	≥ 8.0.0.0 < 9.0.0.10-28sv	9.0.0.10-28sv	NVD
sma 210	—	no fixed version listed	NVD
sma 410	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2gf8-x72h-g57r**NVD** nvd.nist.gov/vuln/detail/CVE-2021-20028**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2021-7491**Additional guidance** psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2021-20028

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