

CVE-2020-5135

SonicWall SonicOS Buffer Overflow Vulnerability

Exigent

CISA KEV since Mar 15, 2022

Actively exploited

Ransomware use known

A buffer overflow vulnerability in SonicOS allows a remote attacker to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a malicious request to the firewall. This vulnerability affected SonicOS Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.

EVRS

85/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.269

98th percentile · FIRST

CISA DEADLINE

Apr 5, 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	0.269 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
sonicos	≤ 6.0.5.3 ≥ 6.5.0.0 ≤ 6.5.1.11 ≥ 6.5.4.0 ≤ 6.5.4.7 7.0.0.0	after 6.0.5.3 · after 6.5.1.11 · after 6.5.4.7	NVD
sonicosv	≤ 6.5.4.4	after 6.5.4.4	NVD

Sources

Vendor guidance github.com/advisories/GHSA-vw5m-894x-7rp4**Additional guidance** psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010**NVD** nvd.nist.gov/vuln/detail/CVE-2020-5135**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2020-26382**Current data** evulnable.com/vulnerability-management/cve/CVE-2020-5135

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