



# CVE-2021-20016

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-20016
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT@sonicwall.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-04 06:15:00 UTC
<b>Updated</b>	2021-02-08 14:40:00 UTC
<b>Description</b>	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform

## Risk And Classification

**EPSS:** 0.780010000 probability, percentile 0.990020000 (date 2026-04-01)

**CISA KEV:** Listed on 2021-11-03; due 2021-11-17; ransomware use Known

**Problem Types:** CWE-89

## CISA Known Exploited Vulnerability

<b>Vendor</b>	SonicWall
<b>Product</b>	SSLVPN SMA100
<b>Name</b>	SonicWall SSLVPN SMA100 SQL Injection Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-20016">https://nvd.nist.gov/vuln/detail/CVE-2021-20016</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 100</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 100</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 100</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 100 Firmware</a>	All	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 200</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 200</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 200</a>	-	All	All	All

Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 200 Firmware</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 200 Firmware</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 210</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 210</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 210</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 210 Firmware</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 210 Firmware</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 400</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 400</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 400</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 400 Firmware</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 400 Firmware</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 410</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 410</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Sma 410</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 410 Firmware</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sma 410 Firmware</a>	-	All	All	All
Application	<a href="#">Sonicwall</a>	<a href="#">Sma 500v</a>	-	All	All	All
Application	<a href="#">Sonicwall</a>	<a href="#">Sma 500v</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Security Advisory	CONFIRM	<a href="https://psirt.global.sonicwall.com">psirt.global.sonicwall.com</a>	Mitigation, Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**