Security Advisory
Vulnerability List
Report Vulnerability
Vulnerability Policy
Hall of Fame
RSS Feed

Vulnerability List

/ Security Advisory / Vulnerability List

SONICWALL SMA100 SSL-VPN AFFECTED BY MULTIPLE VULNERABILITIES

8.8

OVERVIEW

Advisory ID	SNWLID-2025-0011
First Published	2025-05-07
Last Updated	2025-05-08
Workaround	false
Status	Applicable
CVE	CVE-2025-32819, CVE-2025-32820, CVE-2025-32821
CWE	CWE-552, CWE-22, CWE-78
CVSS v3	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Direct Link	

SUMMARY

1) CVE-2025-32819 - Post-Authentication SSLVPN user arbitrary file delete vulnerability

A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN user privileges to bypass the path traversal checks and delete an arbitrary file potentially resulting in a reboot to factory default settings.

CVSS Score: 8.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE-552: Files or Directories Accessible to External Parties

2) CVE-2025-32820 - Post-Authentication SSLVPN user Path Traversal vulnerability

A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN user privileges can inject a path traversal sequence to make any directory on the SMA appliance writable.

CVSS Score: 8.3
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

3) CVE-2025-32821 - Post-Authentication SSLVPN admin remote command injection vulnerability

A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN admin privileges can with admin privileges can inject shell command arguments to upload a file on the appliance.

CVSS Score: 6.7
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

SonicWall SSL VPN SMA1000 series products are not affected by these vulnerabilities.

SonicWall strongly advises users of the SMA 100 series products (SMA 200, 210, 400, 410, and 500v) to upgrade to the mentioned fixed release version to address these vulnerabilities.

AFFECTED PRODUCT(S)

Affected Product(s)	Affected Versions

SMA 100 Series *(SMA 200, 210, 400, 410, 500v)*	10.2.1.14-75sv and earlier versions.

SonicWall SSL VPN SMA1000 series products are not affected by these vulnerabilities.

CPE(S)

WORKAROUND

FIXED SOFTWARE

Fixed Product(s)	Fixed Versions
SMA 100 Series *(SMA 200, 210, 400, 410, 500v)*	10.2.1.15-81sv and higher versions.

COMMENTS

1) Enable multifactor authentication (MFA) as a safety measure.

- MFA has an invaluable safeguard against credential theft and is a key measure of good security posture.

- MFA is effective whether it is enabled on the appliance directly or on the directory service in your organization.

2) Enable WAF on SMA100.

Note: SMA100 devices updated with the fixed firmware version 10.2.1.15-81sv or latest release version are not vulnerable to CVE-2025-32819, CVE-2025-32820, CVE-2025-32821 exploitation. SonicWall PSIRT recommends that customers review their SMA devices to ensure no unauthorized logins.

CREDIT(S)

Rapid7 - Ryan Emmons

REVISION HISTORY

Version

1.0

Date

07-May-2025

Description

Initial Release.

Version

1.1

REFERENCE(S)