Security Advisory

Vulnerability List

SONICWALL SMA1000 SERIES APPLIANCES AFFECTED BY MULTIPLE VULNERABILITIE

7.2

OVERVIEW

Advisory ID	SNWLID-2026-0003
First Published	2026-04-08
Last Updated	2026-04-08
Workaround	false
Status	Applicable
CVE	CVE-2026-4112, CVE-2026-4113, CVE-2026-4114, CVE-2026-4116
CWE	CWE-89, CWE-204, CWE-176
CVSS v3	7.2
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Direct Link	

SUMMARY

1) CVE-2026-4112 - Privilege Escalation via SQL Injection

Improper neutralization of special elements used in an SQL command (“SQL Injection”) in SonicWall SMA1000 series appliances allows a remote authenticated attacker with read-only administrator privileges to escalate privileges to primary administrator.

CVSS Score: 7.2
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2) CVE-2026-4113 - Authentication Response Discrepancy Allows User Credential Enumeration

An observable response discrepancy vulnerability in the SonicWall SMA1000 series appliances allows a remote attacker to enumerate SSL VPN user credentials.

CVSS Score: 5.3
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE-204: Observable Response Discrepancy

3) CVE-2026-4114 - Unicode Possible AMC TOTP Bypass vulnerability

Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN admin to bypass AMC TOTP authentication.

CVSS Score: 6.6
CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
CWE-176: Improper Handling of Unicode Encoding

4) CVE-2026-4116 - Unicode Possible Workplace/Connect Tunnel TOTP Bypass vulnerability

Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN user to bypass Workplace/Connect Tunnel TOTP authentication.

CVSS Score: 6.0
CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L
CWE-176: Improper Handling of Unicode Encoding

SonicWall strongly advises users of the SMA1000 series appliances to upgrade to the mentioned fixed release version to address these vulnerabilities.

There is currently no evidence any of the vulnerabilities addressed in this release are being exploited in the wild. Please note

AFFECTED PRODUCT(S)

Affected Product	Affected Version(s)
SMA1000	12.4.3-03245 (platform-hotfix) and earlier versions. 12.5.0-02283 (platform-hotfix) and earlier versions.

Note: This vulnerability does not affect SSL-VPN running on SonicWall firewalls.

The latest platform-hotfix is available for download on mysonicwall.com

CPE(S)

WORKAROUND

None.

FIXED SOFTWARE

Fixed Product	Fixed Version(s)
SMA1000	12.4.3-03387 (platform-hotfix) and higher versions. 12.5.0-02624 (platform-hotfix) and higher versions.

COMMENTS

CREDIT(S)

CVE-2026-4112 - Anthony Cihan

CVE-2026-4113 - Danti Gionatan

CVE-2026-4114 - Philip Boldt

CVE-2026-4116 - Philip Boldt

REVISION HISTORY

Version

1.0

Date

08-Apr-2026

Description

Initial Release.

REFERENCE(S)