Security Advisory

Vulnerability List

SONICWALL EMAIL SECURITY AFFECTED BY MULTIPLE VULNERABILITIES

3.8

OVERVIEW

Advisory ID	SNWLID-2026-0002
First Published	2026-03-31
Last Updated	2026-03-31
Workaround	false
Status	Applicable
CVE	CVE-2026-3468, CVE-2026-3469, CVE-2026-3470
CWE	CWE-79, CWE-400, CWE-20
CVSS v3	3.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
Direct Link	

SUMMARY

1) CVE-2026-3468 - Stored Cross-Site Scripting (XSS) Vulnerability

A stored Cross-Site Scripting (XSS) vulnerability has been identified in the SonicWall Email Security appliance due to improper neutralization of user-supplied input during web page generation, allowing a remote authenticated attacker as admin user to potentially execute arbitrary JavaScript code.

CVSS Score: 3.5
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

2) CVE-2026-3469 - Denial of Service (DoS) via Malformed Input

A denial-of-service (DoS) vulnerability exists due to improper input validation in the SonicWall Email Security appliance, allowing a remote authenticated attacker as admin user to cause the application to become unresponsive.

CVSS Score: 2.7
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L
CWE-20 – Improper Input Validation

3) CVE-2026-3470 - Lack of Proper Input Sanitization leading to data corruption

A vulnerability exists in the SonicWall Email Security appliance due to improper input sanitization that may lead to data corruption, allowing a remote authenticated attacker as admin user could exploit this issue by providing crafted input that corrupts application database.

CVSS Score: 3.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
CWE-20 – Improper Input Validation

SonicWall strongly advises users of the Email Security products (ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V) 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.

AFFECTED PRODUCT(S)

Affected Product(s)	Affected Versions

Email Security *(ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V)*	10.0.34.8215, 10.0.34.8223 and earlier versions.

CPE(S)

WORKAROUND

None.

FIXED SOFTWARE

Fixed Product(s)	Fixed Versions
Email Security *(ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V)*	10.0.35.8405 and higher versions.

COMMENTS

CREDIT(S)

Brian Mariani of DigitalCanion SA - www.digitalcanion.com

REVISION HISTORY

Version	Date	Description
1.0	31-Mar-2026	Initial Release.

REFERENCE(S)