



# Vulnerability List

🏠 / Security Advisory / Vulnerability List



Security Advisory



Vulnerability List



Report Vulnerability



Vulnerability Policy



Hall of Fame



RSS Feed



SONICWALL EMAIL SECURITY AFFECTED BY MULTIPLE VULNERABILITIES

3.8

## OVERVIEW

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

## 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
---------------------	-------------------

<b>Email Security</b> (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
<b>Email Security</b> (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](http://www.digitalcanion.com)

---

**REVISION HISTORY**

Version

1.0

Date

31-Mar-2026

Description

Initial Release.

---

**REFERENCE(S)**