



# CVE-2026-3470

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

## Summary

<b>CVE</b>	CVE-2026-3470
<b>State</b>	PUBLISHED
<b>Assigner</b>	sonicwall
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 21:16:33 UTC
<b>Updated</b>	2026-04-01 14:23:37 UTC
<b>Description</b>	A vulnerability exists in the SonicWall Email Security appliance due to improper input sanitization that may lead to data corr

## Risk And Classification

**Primary CVSS:** v3.1 3.8 LOW from ADP

**CVSS:** 3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L

**EPSS:** 0.001140000 probability, percentile 0.301010000 (date 2026-04-01)

**Problem Types:** CWE-20 | CWE-20 CWE-20 Improper input validation

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	3.8	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	3.8	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">SonicWall</a>	<a href="#">Email Security</a>	affected 10.0.34.8215 and earlier versions	Linux, Windows
CNA	<a href="#">SonicWall</a>	<a href="#">Email Security</a>	affected 10.0.34.8223 and earlier versions	Linux, Windows

### References

Reference	Source	Link	Tags
<a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0002">psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0002</a>	<a href="mailto:PSIRT@sonicwall.com">PSIRT@sonicwall.com</a>	<a href="https://psirt.global.sonicwall.com">psirt.global.sonicwall.com</a>	
CVE Program record	<a href="https://cve.org">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="https://nvd.nist.gov">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** [Brian Mariani of DigitalCanion SA - www.digitalcanion.com \(en\)](#)

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](#)