CVE-2026-3468

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3468
State	PUBLISHED
Assigner	sonicwall
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 21:16:32 UTC
Updated	2026-04-01 14:23:37 UTC
Description	A stored Cross-Site Scripting (XSS) vulnerability has been identified in the SonicWall Email Security appliance due to improc

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from ADP

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

EPSS: 0.000430000 probability, percentile 0.130380000 (date 2026-04-01)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SonicWall	Email Security	affected 10.0.34.8215 and earlier versions	Linux, Windows
CNA	SonicWall	Email Security	affected 10.0.34.8223 and earlier versions	Linux, Windows

References

Reference	Source	Link	Tags
psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0002	PSIRT@sonicwall.com	psirt.global.sonicwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.