CVE-2026-4116

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4116
State	PUBLISHED
Assigner	sonicwall
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 15:16:14 UTC
Updated	2026-04-13 19:16:52 UTC
Description	Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN u

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from ADP

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

EPSS: 0.001380000 probability, percentile 0.338690000 (date 2026-04-15)

Problem Types: CWE-176 | CWE-176 CWE-176 Improper handling of unicode encoding

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SonicWall	SMA1000	affected 12.4.3-03245 (platform-hotfix) and earlier versions.	Linux
CNA	SonicWall	SMA1000	affected 12.5.0-02283 (platform-hotfix) and earlier versions.	Linux

References

Reference	Source	Link	Tags
psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0003	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

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.