HTML injection in in Time Machine functionality in Guardian/CMC before 25.5.0

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

Summary

CVE	CVE-2025-40891
State	PUBLISHED
Assigner	Nozomi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-18 14:15:59 UTC
Updated	2026-04-14 10:16:26 UTC
Description	A Stored HTML Injection vulnerability was discovered in the Time Machine Snapshot Diff functionality due to improper valid

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from prodsec@nozominetworks.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000400000 probability, percentile 0.122150000 (date 2026-04-15)

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

Version	Source	Type	Score	Severity	Vector
4.0	prodsec@nozominetworks.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:I
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:I
3.1	nvd@nist.gov	Primary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	prodsec@nozominetworks.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nozominetworks	Cmc	All	All	All	All

Application	Nozominetworks	Guardian	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nozomi Networks	Guardian	affected 25.5.0 semver	Not specified
CNA	Nozomi Networks	CMC	affected 25.5.0 semver	Not specified
ADP	Siemens	RUGGEDCOM APE1808	affected * custom	Not specified

References

Reference	Source	Link	Tags
security.nozominetworks.com/NN-2025:12-01	prodsec@nozominetworks.com	security.nozominetworks.com	Vend
cert-portal.siemens.com/productcert/html/ssa-827968.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

Vendor Comments And Credit

Discovery Credit

CNA: This issue was found by Stefano Libero and Andrea Palanca of Nozomi Networks Product Security team during an internal investigation. (en)

Additional Advisory Data

Solutions

CNA: Upgrade to v25.5.0 or later.

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