Stored Cross-Site Scripting (XSS) in Assets and Nodes in Guardian/CMC before 26.0.0

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

Summary

CVE	CVE-2025-40899
State	PUBLISHED
Assigner	Nozomi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 09:16:30 UTC
Updated	2026-05-12 13:17:19 UTC
Description	A Stored Cross-Site Scripting vulnerability was discovered in the Assets and Nodes functionality due to improper validation

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from prodsec@nozominetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:H/VA:H/SC:L/SI:L/SA:L/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: 0.000350000 probability, percentile 0.102610000 (date 2026-05-12)

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
4.0	prodsec@nozominetworks.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:H/VA:H/SC:L/SI:L/
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:H/VA:H/SC:L/SI:L/
3.1	prodsec@nozominetworks.com	Secondary	8.9	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H
3.1	CNA	CVSS	8.9	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

Low

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:H/VA:H/SC:L/SI:L/SA:L/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

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nozomi Networks	Guardian	affected 26.0.0 semver	Not specified
CNA	Nozomi Networks	CMC	affected 26.0.0 semver	Not specified

ADP	Siemens	RUGGEDCOM APE1808	affected * custom	Not specified

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/html/ssa-827968.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
security.nozominetworks.com/NN-2026:2-01	prodsec@nozominetworks.com	security.nozominetworks.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 Andrea Palanca of Nozomi Networks Product Security team during an internal investigation. (en)

Additional Advisory Data

Solutions

CNA: Upgrade to v26.0.0 or later.

Workarounds

CNA: Use internal firewall features to limit access to the web management interface.

CNA: Review all accounts with access to it and delete unnecessary ones.

CNA: Review existing custom fields.

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