



# 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

<b>CVE</b>	CVE-2025-40899
<b>State</b>	PUBLISHED
<b>Assigner</b>	Nozomi
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 09:16:30 UTC
<b>Updated</b>	2026-05-12 13:17:19 UTC
<b>Description</b>	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/MSX/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/MSX/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

### References

Reference	Source	Link	Tags
<a href="https://cert-portal.siemens.com/productcert/html/ssa-827968.html">cert-portal.siemens.com/productcert/html/ssa-827968.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
<a href="https://security.nozominetworks.com/NN-2026:2-01">security.nozominetworks.com/NN-2026:2-01</a>	prodsec@nozominetworks.com	<a href="https://security.nozominetworks.com">security.nozominetworks.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)