Stored Cross-Site Scripting (XSS) in Reports in Guardian/CMC before 25.5.0

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

Summary

CVE	CVE-2025-40892
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 10:16:27 UTC
Description	A Stored Cross-Site Scripting vulnerability was discovered in the Reports functionality due to improper validation of an input

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: 0.000510000 probability, percentile 0.155600000 (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	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	nvd@nist.gov	Primary	8.9	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H
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

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
cert-portal.siemens.com/productcert/html/ssa-827968.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
security.nozominetworks.com/NN-2025:13-01	prodsec@nozominetworks.com	security.nozominetworks.com	Mitig
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 of Nozomi Networks Product Security team during an internal investigation. (en)

Additional Advisory Data

Solutions

CNA: Upgrade to v25.5.0 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 report templates.

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

site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report