



Product Security
INCIDENT RESPONSE TEAM

[PSIRT Policy](#)
[PSIRT GPG Key](#)
[Alerts](#)
[RSS Feed](#)

NN-2026:2-01

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

Last update: 2026-04-15

[CSAF](#)

Advisory ID	NN-2026:2-01
Topic	Stored Cross-Site Scripting (XSS) in Assets and Nodes in Guardian/CMC before 26.0.0
CWE Impact	CWE-79: Improper Neutralization of Input During Generation ('Cross-site Scripting')
Issue date	2026-04-15
Affects	Guardian, CMC < v26.0.0
CVE Name(s)	CVE-2025-40899
CVSS Details	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:H/ CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H
CVSS Score	7.1 (CVSS v4.0) 8.9 (CVSS v3.1)
CVE Risk Level	High (CVSS v4.0) High (CVSS v3.1)
Risk Level for Nozomi customers	High

Summary

A Stored Cross-Site Scripting vulnerability was discovered in the Assets and Nodes functionality due to improper validation of an input parameter.

Impact

An authenticated user with custom fields privileges can define a malicious custom field containing a JavaScript payload. When the victim views the Assets or Nodes pages, the XSS executes in their browser context, allowing the attacker to perform unauthorized actions as the victim, such as modify application data, disrupt application availability, and access limited sensitive information.

Affected Products

Guardian, CMC < v26.0.0

Workarounds and Mitigations

Use internal firewall features to limit access to the web management interface. Review all accounts with access to it and delete unnecessary ones. Review existing custom fields.

Solutions

Upgrade to v26.0.0 or later.

Modification History

2026-04-15: Initial revision

Related Links

[Mitre CVE entry](#)

Acknowledgements

We thank the following parties for their efforts:

- Andrea Palanca of Nozomi Networks Product Security team for finding this issue during an internal investigation

Contact

Nozomi Networks Product Security team can be reached at prodsec@nozominetworks.com.

More contact details on the [PSIRT page](#).

nozominetworks.com © 2020-2026 Nozomi Networks Inc. All rights reserved.

