NN-2026:1-01

Incorrect authorization for Threat Intelligence in Guardian/CMC before 26.0.0

Last update: 2026-04-15

CSAF

Advisory ID	NN-2026:1-01
Topic	Incorrect authorization for Threat Intelligence in G 26.0.0
CWE Impact	CWE-863: Incorrect Authorization
Issue date	2026-04-15
Affects	Guardian, CMC < v26.0.0
CVE Name(s)	CVE-2025-40897
CVSS Details	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/ CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
CVSS Score	7.2 (CVSS v4.0) 8.1 (CVSS v3.1)
CVE Risk Level	High (CVSS v4.0) High (CVSS v3.1)
Risk Level for Nozomi customers	High

Summary

An access control vulnerability was discovered in the Threat Intelligence functionality due to a specific access restriction not being properly enforced for users with view-only privileges.

Impact

An authenticated user with view-only privileges for the Threat Intelligence functionality can perform administrative actions on it, altering the rules configuration, and/or affecting their availability.

Affected Products

Guardian, CMC < v26.0.0

Workarounds and Mitigations

Remove or revoke access to Threat Intelligence users with view-only privileges until a fix is applied.

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.