



Product Security  
INCIDENT RESPONSE TEAM

[PSIRT Policy](#)

[PSIRT GPG Key](#)

[Alerts](#)

[RSS Feed](#)

NN-2026:1-01

# Incorrect authorization for Threat Intelligence in Guardian/CMC before 26.0.0

Last update: 2026-04-15

[CSAF](#)

<b>Advisory ID</b>	NN-2026:1-01
<b>Topic</b>	Incorrect authorization for Threat Intelligence in C 26.0.0
<b>CWE Impact</b>	CWE-863: Incorrect Authorization
<b>Issue date</b>	2026-04-15
<b>Affects</b>	Guardian, CMC < v26.0.0
<b>CVE Name(s)</b>	CVE-2025-40897
<b>CVSS Details</b>	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
<b>CVSS Score</b>	7.2 (CVSS v4.0) 8.1 (CVSS v3.1)
<b>CVE Risk Level</b>	High (CVSS v4.0) High (CVSS v3.1)
<b>Risk Level for Nozomi customers</b>	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](mailto:prodsec@nozominetworks.com).

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

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

