Nozomi Guardian: CVE-2025-40897

Overview

On April 15, 2026, Broadcom published CVE-2025-40897 detailing an access control vulnerability in Nozomi Guardian's Threat Intelligence module.

Affected Products and Versions

Nozomi Guardian < 26.0.0

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2026-40897	8.1 (High)	Not Affected	Guardian	Incorrect Authorization (CWE-863)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

This vulnerability enables users of the Threat Intelligence module with view-only privileges to make administrative changes to the device. For Gas Power Controls customers, view-only privileged users are not created as part of the standard configuration, so customer equipment is unaffected unless additional view-only users have been created on the Guardian device.

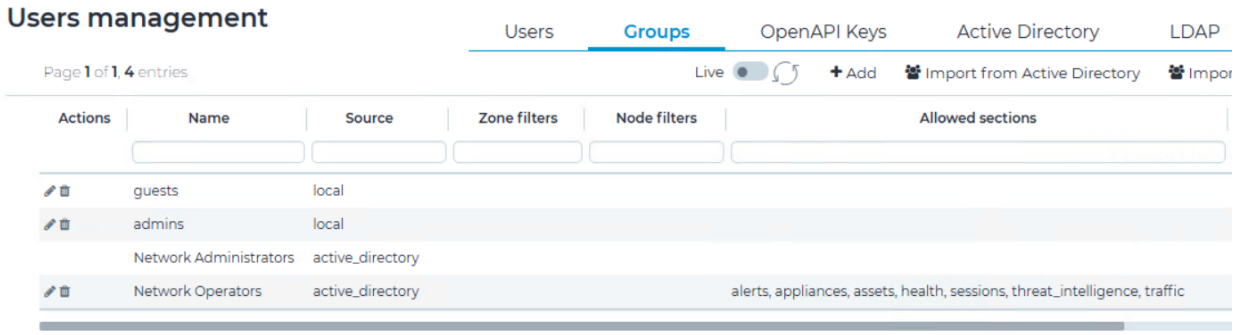
Exploitation Status

GE Vernova has not yet observed or received any reports that Gas Power customer equipment has been compromised due to this vulnerability.

Remediation/Mitigation (Gas Power Customers)

If view-only users have been created on a Guardian device, then the equipment can be affected by this vulnerability. The following steps may be performed to mitigate the vulnerability:

1. Remove Threat Intelligence View Only Permission
    a. Log into a device that can access IDS
    b. Navigate to the IDS using a browser
    c. Log in using the Nozomi administration account.
    d. Go to "Administration (Gear Icon Top Left) -> System -> Users -> Groups

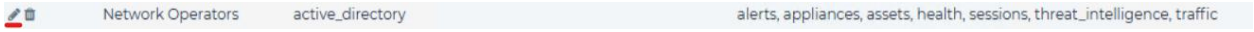


© 2026 GE Vernova. All rights reserved. GE Vernova reserves the right to vary its findings and conclusions should any information or technical knowledge come to GE after the date of this document. This Security Advisory does not vary any contractual relationship between GE Vernova and its customer. NO REPRESENTATION OR WARRANTY IS MADE OR IMPLIED AS TO ITS COMPLETENESS, ACCURACY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

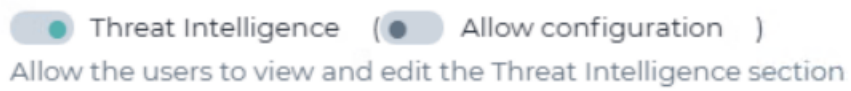
NOTE: Look through the allowed sections column for “threat_intelligence” permission.
If “threat_intelligence” permission is found in any group, follow the steps below.
If not, move to step 10.

e. Select the pencil icon beside the affected group.

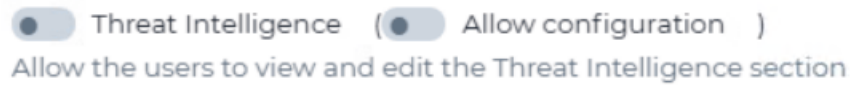
NOTE: If there is no pencil icon, check the other Nozomi devices. Only the Nozomi device that created the group can edit it.



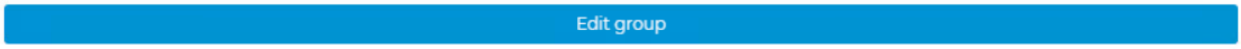
f. Scroll down to the Threat Intelligence section



g. Uncheck the Threat Intelligence



h. Select the "Edit group" button at the bottom to save



i. Repeat for all groups that have the “threat_intelligence” permission in the allowed sections column
j. Repeat to check each Nozomi device

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or incident/vulnerability reporting: https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	5/26/2026	Initial Release

Disclaimer

GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Any rights and remedies arising out of or in connection with this Security Notice are subject to the applicable terms of a GE Vernova contract

© 2026 GE Vernova. All rights reserved. GE Vernova reserves the right to vary its findings and conclusions should any information or technical knowledge come to GE after the date of this document. This Security Advisory does not vary any contractual relationship between GE Vernova and its customer. NO REPRESENTATION OR WARRANTY IS MADE OR IMPLIED AS TO ITS COMPLETENESS, ACCURACY, OR FITNESS FOR ANY PARTICULAR PURPOSE.