GE Vernova
Steam Power
Nuclear P&L

April 12, 2024 **CYBERSECURITY**

Topic: Nozomi – Multiple Vulnerabilities

Overview

Nozomi has published via their Web site – Product Security Incident Response Portal - several security bulletins linked to the products Guardian/CMC.

- NN-2023:12-01 (16/01/2024) - Check Point IoT integration: WebSocket returns assets data without authentication in Guardian/CMC before 23.3.0
  https://security.nozominetworks.com/NN-2023:12-01/

- NN-2024:1-01 (10/04/2024) – DoS on IDS parsing of malformed Radius packets in Guardian before 23.4.1
  https://security.nozominetworks.com/NN-2024:1-01/

- NN-2023:17-01 (11/04/2024) – Information disclosure via audit records for OpenAPI requests in Guardian/CMC before 23.4.1
  https://security.nozominetworks.com/NN-2023:17-01/

Affected Products and Versions:

- NN-2023:12-01 => Guardian, CMC < v23.3.0
- NN-2024:1-01 => Guardian < v23.4.1
- NN-2023:17-01 => Guardian, CMC < v23.4.1

NN-2023:12-01 - **CVE-2023-5253**
Impact : Malicious unauthenticated users with knowledge on the underlying system may be able to extract asset information

NN-2024:1-01 - **CVE-2024-0218**
Impact: Network traffic may not be analyzed until the IDS module is restarted.

NN-2023:17-01 - **CVE-2023-6916**
Impact: Unauthorized access, privilege escalation.

Remediation / Mitigation

Referring to each security bulletin:

- NN-2023:12-01
  Workarounds and Mitigations
  Use internal firewall features to limit access to the web management interface
  Solutions
  Upgrade to v23.3.0 or later.

- NN-2024:1-01
  Workarounds and Mitigations
  N/A
  Solutions
  Upgrade to v23.4.1 or later.

- NN-2023:17-01
  Workarounds and Mitigations
  Nozomi Networks recommends creating specific users for OpenAPI usage, with only the necessary permissions to access the required data sources. Additionally, it is advised to limit API keys to allowed IP addresses whenever possible. Finally, it is also suggested to regenerate existing API keys periodically and to review sign-ins via API keys in the audit records.
  Solutions
  Upgrade to v23.4.1 or later.

Reminder

it is mandatory, as a security rule, to keep the Nozomi devices fully operational from security perspective and to respect following practices

- Firmware & General Updates Support contracts should be subscribed
- Firmware should be updated regularly.

Defense-in-depth

To minimize the risk of the exploitation of current and future system vulnerabilities, GE Steam Power highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

GE Vernova
Steam Power
Nuclear P&L

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your GE Power Automation & Controls salesperson or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com for help with ordering cybersecurity services and solutions.

Thierry PELET
Product Security Leader, GE Steam Power – Nuclear P&L
thierry.pelet@ge.com

Revision History

Version	Release Date	Purpose
A	April 12, 2024	Initial version