SSA-647455: Multiple Vulnerabilities in Nozomi Guardian/CMC before 22.6.2 on RUGGEDCOM APE1808 devices

Publication Date: 2023-10-10
Last Update: 2023-11-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.1

SUMMARY

Nozomi Networks has published information on vulnerabilities in Nozomi Guardian/CMC before V22.6.2. This advisory lists the related Siemens Industrial products affected by these vulnerabilities.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available. Customers are advised to consult and implement the workarounds provided in Nozomi Network's upstream security notifications.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808: All versions with Nozomi Guardian / CMC before V22.6.2	Contact customer support to receive patch and update information. See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Use internal firewall features to limit access to the web management interface
- Adopt best practices that include closing the browser after a logout

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The RUGGEDCOM APE1808 is a powerful utility-grade application hosting platform that lets you deploy a range of commercially available applications for edge computing and cybersecurity in harsh, industrial environments.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-22378

A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the sorting parameter, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application.

Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2023-22843

An authenticated attacker with administrative access to the appliance can inject malicious JavaScript code inside the definition of a Threat Intelligence rule, that will later be executed by another legitimate user viewing the details of such a rule.

An attacker may be able to perform unauthorized actions on behalf of legitimate users. JavaScript injection was possible in the content for Yara rules, while limited HTML injection has been proven for packet and STYX rules. The injected code will be executed in the context of the authenticated victim's session.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2023-23574

A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the alerts_count component, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application.

Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2023-23903

An authenticated administrator can upload a SAML configuration file with the wrong format, with the application not checking the correct file format. Every subsequent application request will return an error.

The whole application in rendered unusable until a console intervention.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-24015

A partial DoS vulnerability has been detected in the Reports section, exploitable by a malicious authenticated user forcing a report to be saved with its name set as null.

The reports section will be partially unavailable for all later attempts to use it, with the report list seemingly stuck on loading.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-24471

An access control vulnerability was found, due to the restrictions that are applied on actual assertions not being enforced in their debug functionality.

An authenticated user with reduced visibility can obtain unauthorized information via the debug functionality, obtaining data that would normally be not accessible in the Query and Assertions functions.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2023-24477

In certain conditions, depending on timing and the usage of the Chrome web browser, Guardian/CMC versions before 22.6.2 do not always completely invalidate the user session upon logout. Thus an authenticated local attacker may gain acces to the original user's session.

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-384: Session Fixation

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-10-10): Publication date
V1.1 (2023-11-14): Added solution for affected products

TERMS OF USE