SSA-292063: Multiple Vulnerabilities in Nozomi Guardian/CMC before 22.6.3 and 23.1.0 on RUGGEDCOM APE1808 devices

Publication Date:	2023-11-14
Last Update:	2024-05-14
Current Version:	V1.1
CVSS v3.1 Base Score:	8.1

SUMMARY

Nozomi Networks has published information on vulnerabilities in Nozomi Guardian/CMC before V22.6.3 and 23.1.0. 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 V22.6.3 or 23.1.0 affected by all CVEs	Upgrade Nozomi Guardian / CMC to V23.4.1. 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:

- CVE-2023-2567: Use internal firewall features to limit access to the web management interface
- CVE-2023-32649: It is recommended to monitor the IDS log to check for abnormal stops and restarts

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-2567

A SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in certain parameters used in the Query functionality, 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	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/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-2023-29245

A SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in certain fields used in the Asset Intelligence functionality of our IDS, may allow an unauthenticated attacker to execute arbitrary SQL statements on the DBMS used by the web application by sending specially crafted malicious network packets.

Malicious users with extensive knowledge on the underlying system may be able to extract arbitrary information from the DBMS in an uncontrolled way, or to alter its structure and data.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2023-32649

A Denial of Service (Dos) vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in certain fields used in the Asset Intelligence functionality of our IDS, allows an unauthenticated attacker to crash the IDS module by sending specially crafted malformed network packets.

During the (limited) time window before the IDS module is automatically restarted, network traffic may not be analyzed.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

Nozomi provides a public RSS feed for their security alerts to which customers can also subscribe [1].

[1] https://security.nozominetworks.com/alerts/

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 (2023-11-14):	Publication Date
V1.1 (2024-05-14):	Added specific product version to remediations

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.