

SSA-320629: Security Vulnerabilities Fixed in RUGGEDCOM CROSSBOW V5.3

Publication Date: 2023-03-14
Last Update: 2023-03-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

RUGGEDCOM CROSSBOW before V5.3 contains two vulnerabilities that could allow authenticated remote attackers to access data they are not authorized for, or execute arbitrary database queries via an SQL injection attack.

Siemens has released an update for RUGGEDCOM CROSSBOW and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM CROSSBOW: All versions < V5.3	Update to V5.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109813558/

WORKAROUNDS AND MITIGATIONS

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

RUGGEDCOM CROSSBOW is a secure access management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices.

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-2023-27462

The client query handler of the affected application fails to check for proper permissions for specific read queries. This could allow authenticated remote attackers to access data they are not authorized for.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2023-27463

The audit log form of affected applications is vulnerable to SQL injection. This could allow authenticated remote attackers to execute arbitrary SQL queries on the server database.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/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')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Cameron Whitehead from RISES Center at UCF for reporting the vulnerability CVE-2023-27463

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 (2023-03-14): Publication Date

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.