SSA-472630: Security Vulnerabilities Fixed in RUGGEDCOM CROSSBOW V5.4

Publication Date: 2023-08-08
Last Update: 2023-08-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The RUGGEDCOM CROSSBOW server application before V5.4 contains multiple vulnerabilities that could allow an attacker to execute arbitrary database queries via SQL injection attacks, to create a denial of service condition, or to write arbitrary files to the application's file system.

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 < V5.4	Update to V5.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109822716/

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-2021-31239

An issue found in SQLite SQLite3 v.3.35.4 that could allow a remote attacker to cause a denial of service via the appendvfs.c function.

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-125: Out-of-bounds Read

Vulnerability CVE-2022-37971

Microsoft Windows Defender Elevation of Privilege Vulnerability. An attacker who successfully exploited this vulnerability could gain specific limited SYSTEM privileges. This vulnerability could allow an attacker to delete data that could include data that results in the service being unavailable.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2023-27411

The affected applications is vulnerable to SQL injection. This could allow an authenticated remote attackers to execute arbitrary SQL queries on the server database and escalate privileges.

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')

Vulnerability CVE-2023-37372

The affected applications is vulnerable to SQL injection. This could allow an unauthenticated remote attackers to execute arbitrary SQL queries on the server database.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/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-2023-37373

The affected applications accept unauthenticated file write messages. An unauthenticated remote attacker could write arbitrary files to the affected application's file system.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- The UK's National Cyber Security Centre (NCSC) for reporting the vulnerabilities CVE-2023-27411, CVE-2023-37372, and CVE-2023-37373

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 (2023-08-08): Publication date

TERMS OF USE