TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-04-25
DOC. IDENTIFIER: 8DBD000153
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities in Hitachi Energy's RTU500 Series Product

CVE-2022-23937
CVE-2022-0778
CVE-2021-3711
CVE-2021-3712

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of multiple reported vulnerabilities in the Wind River VxWorks and the OpenSSL that affects the RTU500 series. Successful exploitation may crash the RTU, causing a denial-of-service. The product versions listed in this document are affected by the vulnerabilities as elaborated in the Section Vulnerability ID, Severity and Details. For immediate mitigation/workaround information, please refer to the General Mitigation Factors/Workarounds.

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2022-23937 Detail CVSS v3.1 Base Score: 7.5 HIGH CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here CWE-125: Out-of-bounds Read	A vulnerability exists in the Wind River VxWorks version 6.9 that affects the RTU500 series product versions listed below. An attacker could exploit the vulnerability by using a specific crafted packet that may lead to an out-of-bounds read during an IKE initial exchange scenario.
CVE-2022-0778 Detail CVSS v3.1 Base Score: 7.5 HIGH CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	A vulnerability exists in the OpenSSL version 1.0.2 that affects the RTU500 Series product versions listed below. An attacker can exploit the BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli.
CVE-2021-3711 Detail CVSS v3.1 Base Score: 9.8 CRITICAL CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	A vulnerability exists in the OpenSSL Version 1.0.2 that affects the RTU500 Series product versions listed below. An attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behavior or causing the application to crash.
CVE-2021-3712 Detail CVSS v3.1 Base Score: 7.4 HIGH CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H Link to NVD: click here CWE-125: Out-of-bounds Read	A vulnerability exists in the OpenSSL Version 1.0.2 that affects the RTU500 Series product versions listed below. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions, then this issue could be hit. This might result in a crash (causing a Denial-of-Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Affected Product Versions & Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

CVE IDs	Affected Version	Recommended Actions
CVE-2022-23937 CVE-2022-0778 CVE-2021-3711 CVE-2021-3712	RTU500 series CMU Firmware all versions	Follow General Mitigation Factors
	RTU500 series CMU Firmware version 12.0.1 – 12.0.14	Update to CMU Firmware version 12.0.15*
	RTU500 series CMU Firmware version 12.2.1 – 12.2.11	Update to CMU Firmware version 12.2.12*
	RTU500 series CMU Firmware version 12.4.1 – 12.4.11	Update to CMU Firmware version 12.4.12*
	RTU500 series CMU Firmware version 12.6.1 – 12.6.8	Update to CMU Firmware version 12.6.9*
	RTU500 series CMU Firmware version 12.7.1 – 12.7.5	Update to CMU Firmware version 12.7.6*
	RTU500 series CMU Firmware version 13.2.1 – 13.2.5	Update to CMU Firmware version 13.2.6*
	RTU500 series CMU Firmware version 13.3.1 – 13.3.3	Update to CMU Firmware version 13.3.4*
	RTU500 series CMU Firmware version 13.4.1	Update to CMU Firmware version 13.4.2

Hitachi Energy recommends that customers apply the update at the earliest convenience.

*Planned

General Mitigation Factors/Workarounds

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Frequently Asked Questions

What is RTU500 series?

RTU500 series, consists of RTU520, RTU530, RTU540 and RTU560 products.

These are remote terminal units configurable to nearly all demands made on remote stations in networks for electrical substations, gas, oil, water, and district heating.

The RTU500 series therefore provides a flexible and modular design with many integrated functionalities covering a wide range of individual solutions suitable for transmission, distribution substations, smart grid, or feeder automation applications.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability remotely. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, these vulnerabilities have been publicly disclosed by the respective Open-Source Software.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

No, at the date of this advisory publication Hitachi Energy had not received any information indicating that these vulnerabilities have been exploited.

Support

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2023-04-25	1	Initial public release.

DocuSigned by: