REVISION: B
PUBLICATION DATE: 2021-12-02
DOC. IDENTIFIER: 8DBD000064
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

OpenSSL and Libxml2 Related Vulnerabilities in Hitachi Energy RTU500 series

CVE-2020-1968
CVE-2020-24977
CVE-2021-3517

Notice

Summary

Hitachi Energy is aware of internal reports of the OpenSSL and libxml2 related vulnerabilities in the RTU500 series versions listed below. Recommended action for each affected version is listed in the Recommended Immediate Actions Section.

An attacker who successfully exploited this vulnerability could eavesdrops on the traffic, retrieve information from memory or to cause a denial-of-service.

Affected Products and Versions

List of affected products and product versions (* indicates all versions – See Recommended Immediate Actions for details):

- RTU500 series CMU Firmware version 11.*
- RTU500 series CMU Firmware version 12.0.*
- RTU500 series CMU Firmware version 12.2.*
- RTU500 series CMU Firmware version 12.4.*
- RTU500 series CMU Firmware version 12.6.*
- RTU500 series CMU Firmware version 12.7.*
- RTU500 series CMU Firmware version 13.0.*
- RTU500 series CMU Firmware version 13.1.*
- RTU500 series CMU Firmware version 13.2.1

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-**2020-1968** CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here	**OpenSSL:** The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite and then eavesdrop on all encrypted communications sent over that TLS connection.
CVE-2020-24977 CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L Link to NVD: click here	**Libxml2:** a global buffer over-read vulnerability in xmlEncodeEntitiesInternal in the affected libxml2/entities.c.
CVE-2021-3517 CVSS v3.1 Base Score: 8.6 High CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H Link to NVD: click here	**Libxml2:** A flaw exists in the xml entity encoding functionality of the affected libxml2. An attacker who can supply a crafted file to be processed by an application could trigger an out-of-bounds read.

The following lists the following possible impact of those vulnerabilities:

– **Decryption of TLS traffic:** Exploitation of the OpenSSL Raccoon attack may allow an attacker to compute the pre-master secret between the client and server in connections which have used a Diffie-Hellman (DH) based ciphersuite.

– **Memory information retrieval and possible application crash:** An attacker with access to the network can exploit the vulnerabilities related to LibXML2 and may retrieve information from the memory. This type of attack may also cause the application to crash causing denial-of-service.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
RTU500 series CMU Firmware version 11.*	This product version is End-of-Life (EOL). Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to a non-affected supported version.
RTU500 series CMU Firmware version 12.0.1 – 12.0.13	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or Update to RTU500 series CMU firmware 12.0.14 (to be released by end-of-February 2022).
RTU500 series CMU Firmware version 12.2.1 – 12.2.10	Update to RTU500 series CMU firmware as of version 12.2.11
RTU500 series CMU Firmware version 12.4.1 – 12.4.10	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or Update to RTU500 series CMU firmware as of version 12.4.11 (to be released by end-of-January 2022).
RTU500 series CMU Firmware version 12.6.1 – 12.6.6	Update to RTU500 series CMU firmware as of version 12.6.7.
RTU500 series CMU Firmware version 12.7.1	Update to RTU500 series CMU firmware as of version 12.7.2
RTU500 series CMU Firmware version 13.0.1 – 13.0.2	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.
RTU500 series CMU Firmware version 13.1.1 – 13.1.2	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.
RTU500 series CMU Firmware version 13.2.1	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy or upgrade to the latest RTU500 series CMU firmware as of version 13.2.3.

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

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 is a remote terminal unit product 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 grids or feeder automation applications.

What might an attacker use the vulnerability to do?

The vulnerabilities as described in this advisory may cause:

- Decryption of TLS traffic which results in traffic eavesdropping
- Memory information retrieval and denial-of-service on RTU500 series.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. 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 teams.

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

No, Hitachi Energy had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

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[1] – cybersecurity@hitachienergy.com .

Revision

Date of the Revision	Revision	Description
2021-11-17	A	Initial public release.
2021-12-02	B	Section Recommended Immediate Actions: • RTU500 series CMU Firmware version 12.6.7 is available.

[1] Signature file of this PDF is available at https://www.hitachienergy.com/cybersecurity/alerts-and-notifications