TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-04-25
DOC. IDENTIFIER: 8DBD000150
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

OpenSSL Vulnerabilities in Hitachi Energy's RTU500 series Product

CVE-2023-0286
CVE-2022-4304

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the vulnerabilities CVE-2023-0286 and CVE-2022-4304 in the OSS component OpenSSL, that affects the RTU500 versions that are listed below. An attacker successfully exploiting these vulnerabilities could retrieve the memory contents remotely, carry out DoS and man-in-the-middle attacks. Please refer to the Recommended Immediate Actions for information about the available mitigation/remediation strategies.

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-2023-0286 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	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.
CVE-2022-4304 Detail CVSS v3.1 Base Score: 5.9 MEDIUM CVSS v3.1 Vector:/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Link to NVD: click here	A timing-based side channel exists in the RSA Decryption implementation which could be sufficient to recover a plaintext across a network. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes. Possible scenario to exploit this vulnerability: In a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

Affected Product Versions & Recommended Immediate Actions

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

Vulnerability ID	Affected Version	Recommended Actions
CVE-2023-0286 CVE-2022-4304	RTU500 series CMU Firmware versions 12.0.1 – 12.0.15 12.2.1 – 12.2.12 12.4.1 – 12.4.12 12.6.1 – 12.6.9 12.7.1 – 12.7.6 13.2.1 – 13.2.6 13.3.1 – 13.3.3 13.4.2	Until the updates are made available, follow the General Mitigation Factors/Workarounds shown below in this document *

Hitachi Energy recommends that customers implement the general mitigation measures as stated in this advisory and apply the updates at the earliest when they are available.

* Updates are 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.

What is the scope of the vulnerability?

An attacker who successfully exploits these vulnerabilities can affect the following functionalities or components in the product.

- CVE-2023-0286: All kind of functionalities using certificates, if certificate revocation is used.
- CVE-2022-4304: TLS connections as used by https, IEC62351-3 based protocols (like IEC 60870-5-104, DNP3)

Could the vulnerability be exploited remotely?

Yes, an attacker through specially crafted packets and messages can retrieve the contents of RTU memory or can insert in between to either cause Denial of Service or replay attacks. 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 minimal number of ports opened as well as having firewall policies to prevent or mitigate the effects of DoS and replay attacks.

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: