REVISION: A
PUBLICATION DATE: 2021-11-17
DOC. IDENTIFIER: 8DBD000063
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Specially Crafted IEC 60870-5-104 Packet Vulnerability in RTU500 series

CVE-2021-35533

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a private report of a vulnerability in the Bidirectional Communication Interface (BCI) IEC 60870-5-104 function of the RTU500 series providing support for bi-directional IEC 60870-5-104 communication. Affected versions are listed below. An update is available that remediates the reported vulnerability.

An attacker could exploit this vulnerability only on RTU500 series in which BCI IEC 60870-5-104 is configured and enabled by project configuration. Note that BCI IEC 60870-5-104 function is disabled (not configured) by default. Sending IEC 60870-5-104 APDUs with wrong length information to an affected product, an attacker could cause the product to reboot.

Affected Products and Versions

List of affected products and product versions (* indicates all versions):

- RTU500 series CMU Firmware version 12.0.*
- RTU500 series CMU Firmware version 12.2.*
- RTU500 series CMU Firmware version 12.4.*

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-2021-35533 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	A vulnerability exists in the BCI IEC 60870-5-104 function included in the product versions listed above. If BCI IEC 60870-5-104 is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500, causing the receiving RTU500 CMU to reboot. The vulnerability is caused by the validation error in the APDU parser of the BCI IEC 60870-5-104 function.

Recommended Immediate Actions

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

Affected Versions	Recommended Actions
RTU500 series CMU firmware version 12.0.* RTU500 series CMU firmware version 12.2.* RTU500 series CMU firmware version 12.4.* (*: all Versions)	- Disable BCI IEC 60870-5-104 function by configuration if it is not used - Update to RTU500 series CMU Firmware version 12.6.5.0 or higher (e.g., RTU500 CMU Firmware version 12.7.* or CMU Firmware version 13.2.* or higher).

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

Mitigation Factors/Workarounds

As the vulnerability affects only the RTU500 series with BCI IEC 60870-5-104 configured and enabled, a possible mitigation is to disable the BCI IEC 60870-5-104 function if it is not used.

By default, the BCI IEC 60870-5-104 is disabled.

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 grid or feeder automation applications.

What is the scope of the vulnerability?

The vulnerability affects only RTU500 series in which BCI IEC 60870-5-104 is configured and enabled by project configuration.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could reboot a RTU500. During the reboot phase, the primary functionality of the attacked RTU500 is not available.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted IEC 60870-5-104 message and sending the message to an affected system node running the BCI IEC 60870-5-104 functionality. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that an attacker installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above

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?

No, Hitachi Energy received information about this vulnerability internally.

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 – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2021-11-17	A	Initial public release.