REVISION: A
PUBLICATION DATE: 2022-06-28
DOC. IDENTIFIER: 8DBD000111
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Modbus File Write Vulnerability in Hitachi Energy's RTU500 series Product

CVE-2022-2081

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of an internally reported vulnerability in the Modbus stack, that affects the RTU500 series. Note that HCI Modbus TCP function is disabled (not configured) by default. 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 HCI Modbus TCP is configured and enabled by project configuration. Sending a specially crafted Modbus TCP packet in a high rate, may cause a stack overflow which results in a reboot of the product.

Affected Products and Versions

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

- RTU500 series CMU Firmware version 12.0.1 – 12.0.14
- RTU500 series CMU Firmware version 12.2.1 – 12.2.11
- RTU500 series CMU Firmware version 12.4.1 – 12.4.11
- RTU500 series CMU Firmware version 12.6.1 – 12.6.7
- RTU500 series CMU Firmware version 12.7.1 – 12.7.3
- RTU500 series CMU Firmware version 13.2.1 – 13.2.4
- RTU500 series CMU Firmware version 13.3.1

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-2022-2081 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-121: Stack-based Buffer Overflow	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function.

Recommended Immediate Actions

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

Affected Versions	Recommended Actions
All versions	Disable HCI Modbus TCP function by configuration if it is not used
RTU500 series CMU firmware version 12.0.1.0 - 12.0.13.0	Update to RTU500 series CMU Firmware version 12.0.14.0 (*), or higher
RTU500 series CMU firmware version 12.2.1.0 – 12.2.11.0	Update to RTU500 series CMU Firmware version 12.2.12.0 (*), or higher
RTU500 series CMU firmware version 12.4.1.0 – 12.4.11.0	Update to RTU500 series CMU Firmware version 12.4.12.0 (*), or higher
RTU500 series CMU firmware version 12.6.1.0 – 12.6.7.0	Update to RTU500 series CMU Firmware version 12.6.8.0 (*), or higher
RTU500 series CMU firmware version 12.7.1.0 – 12.7.3.0	Update to RTU500 series CMU Firmware version 12.7.4.0 (*), or higher
RTU500 series CMU firmware version 13.2.1.0 – 13.2.4.0	Update to RTU500 series CMU Firmware version 13.2.5.0 (*), or higher
RTU500 series CMU firmware version 13.3.1.0	Update to RTU500 series CMU Firmware version 13.3.2.0, or higher

(*: Version planned)

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 HCI Modbus TCP configured and enabled, a possible mitigation is to disable the HCI Modbus TCP function if it is not used.

By default, the HCI Modbus TCP 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 might an attacker use the vulnerability to do?

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

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted Modbus TCP message and sending the message to an affected system node running the HCI Modbus TCP functionality repeatedly. 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 has not received any information indicating that this vulnerability has 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
2022-06-28	A	Initial public release.