

TLP: CLEAR

REVISION: 1
PUBLICATION DATE: 2023-02-14
DOC. IDENTIFIER: 8DBD000132
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

IEC 61850 MMS-Server Vulnerability in Hitachi Energy's RTU500 series Product CVE-2022-3353

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Hitachi Energy or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Hitachi Energy or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Hitachi Energy and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Summary

Hitachi Energy is aware of a reported vulnerability in the IEC 61850 communication stack, that is used in the RTU500 series product versions listed in this document. A version is available that remediates the identified vulnerabilities. By default, the RTU500 series has the IEC 61850 server functionality disabled and is configured/enabled by project requirement. An attacker who successfully exploited this vulnerability could force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. A manual reboot is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections. During the reboot phase, the primary functionality of the device is not available.

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-2022-3353 CVSS v3.1 Base Score: 5.9 Medium CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here	A vulnerability exists in the IEC 61850 communication stack of the RTU500 series product versions listed below. An attacker could exploit the vulnerability by using a specially crafted message sequence to force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. Already existing/established client-server connections are not affected.

Affected Product Versions & Recommended Immediate Actions

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

Affected Version	Recommended Actions
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 – 12.7.4	Update to CMU Firmware version 12.7.5*
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*

*Planned

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 grid, or feeder automation applications.

What is the scope of the vulnerability?

An attacker who successfully exploits this vulnerability can force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. A manual reboot is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections.

Note:

- Already existing/established client-server connections are not affected (will not be disconnected).
- IEC 61850 communication for GOOSE publishing or subscription is not affected.
- New IEC 61850 MMS connections may be affected.
- IEC 61850 client functionality is not affected.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. A manual reboot is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections.

During the reboot phase, the primary functionality of the device is not available.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by using a specially crafted message sequence, to force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. Such attack requires, direct or indirect access to the industrial control system network. Indirect access could be achieved by various means, such as through a misconfigured firewall, penetrating the firewall defence mechanism or by using a compromised system node, infected with a malware capable of replaying the crafted message, but not limited to these means. Recommended practices help to 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 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?

No, this vulnerability has not been publicly disclosed. 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, at the date of this advisory publication Hitachi Energy had not received any information indicating that this vulnerability had 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
2023-02-14	1	Initial public release.

DS

