TLP:CLEAR

REVISION: 1
PUBLICATION DATE: 2023-02-14
DOC. IDENTIFIER: 8DBD000128
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

IEC 61850 MMS-Server Vulnerability in Hitachi Energy's ITT600 SA Explorer Product

CVE-2022-3353

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a reported vulnerability in the IEC 61850 communication stack that, is used in the ITT600 SA Explorer product versions listed in this document. A version is available that remediates the identified vulnerability.

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 restart of simulated IED is required to re-enable IEC 61850 MMS-server communication for accepting new MMS-client connections.

During the restart phase, the primary functionality of the simulated 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 ITT600 SA Explorer 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
ITT600 SA Explorer 1.1.0 ITT600 SA Explorer 1.1.1 ITT600 SA Explorer 1.1.2 ITT600 SA Explorer 1.5.0 ITT600 SA Explorer 1.5.1 ITT600 SA Explorer 1.6.0 ITT600 SA Explorer 1.6.0.1 ITT600 SA Explorer 1.7.0 ITT600 SA Explorer 1.7.2 ITT600 SA Explorer 1.8.0 ITT600 SA Explorer 2.0.1 ITT600 SA Explorer 2.0.2 ITT600 SA Explorer 2.0.3 ITT600 SA Explorer 2.0.4.1 ITT600 SA Explorer 2.0.5.0 ITT600 SA Explorer 2.0.5.4	ITT600 SA Explorer is a testing tool, and it is used only for testing and/or commissioning. For all versions apply General Mitigation Factors/Workarounds.
ITT600 SA Explorer 2.1.0.4 ITT600 SA Explorer 2.1.0.5	ITT600 SA Explorer 2.1 SP1 (2.1.1.2) contains the IEC 61850 stack with the remediation. It is recommended to upgrade to this version.

Hitachi Energy recommends that customers upgrade at the earliest convenience to the latest version.

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 Hitachi Energy ITT600?

Integrated Testing Tool ITT600 SA Explorer is designed for easy diagnosis and troubleshooting of IEC 61850 compliant substation automation systems and applications. It features convenient navigation, comprehensive presentation of application data and support for consistency checks, both on and off-line.

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 restart of simulated IED is required to re-enable 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 restart of simulated IED is required to re-enable IEC 61850 MMS-server communication for accepting new MMS-client connections.

During the restart phase, the primary functionality of the simulated 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