TLP:WHITE

REVISION: 1
PUBLICATION DATE: 2023-02-28
DOC. IDENTIFIER: 8DBD000146
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Update package validation vulnerability in Hitachi Energy's Relion® 670, 650 and SAM600-IO Series Products

CVE-2022-3864

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a report from Nozomi Networks Labs, concerning the vulnerability CVE-2022-3864 affecting the Relion® 670/650/SAM600-IO series versions listed below. Recommended actions for each affected version are listed in the “Recommended Immediate Actions” section of this document.
An attacker who manages to get access with security privileges to the device, can start the update mechanism, supplying a malicious update package to the IED. When the system attempts to verify the tampered update package, a crash occurs resulting in the reboot of the device, after reboot the device is back in normal operation.

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-2022-3864 CVSS v3.1 Base Score: 4.5 - Medium CVSS v3.1 Vector: AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H Link to NVD: click here	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Relion 670/650 series version 2.2.0 all revisions	For all versions apply General Mitigation Factors. Ensure that Field Service Tool access is disabled, and only enable it on an as-needed basis (e.g. planned upgrades). Remediation will be available for all affected versions.
Relion 670/650/SAM600-IO series version 2.2.1 all revisions	
Relion 670 series version 2.2.2 all revisions	
Relion 670 series version 2.2.3 all revisions	
Relion 670/650 series version 2.2.4 all revisions	
Relion 670/650 series version 2.2.5 all revisions	

Whenever applicable, Hitachi Energy recommends that customers apply the update when available.

General Mitigation Factors

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. Proper password policies and processes should be followed.

For detailed instructions on how to disable the “Field Service Tool access”, please follow the referent product Technical Manual.

Frequently Asked Questions

What is Relion 670/650/SAM600-IO Series?

Hitachi Energy Relion 670/650/SAM600-IO series Intelligent Electronic Devices (IEDs) belong to the Relion protection and control product family. This family offers the widest range of products for the protection, control, measurement, and supervision of power systems. To ensure interoperable and future-proof solutions, Relion products have been designed to implement the core values of the IEC 61850 standard.

How could an attacker exploit the vulnerability?

To exploit the vulnerability, an attacker must have authenticated access to the Field Service Update application and be connected to the system. An insider threat or instrumented operator of the device can start the update mechanism supplying a malicious update package to the IED. When the malicious update package is verified, a crash occurs resulting in the reboot of the device.

Could the vulnerability be exploited remotely?

By default, it is recommended to keep the Field Service Tool access disabled, and only enable it when upgrades are planned.
The reported vulnerability can only be exploited, when the Field Service Tool access is enabled, and the attacker has security privilege access to the system and possess a malicious update package.
Additional recommended practices to reduce the risk of exploitation, 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 or could an attacker exploit the vulnerability?

No, Hitachi Energy received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

No, when this security advisory was originally issued, Hitachi Energy had not received any information indicating that these vulnerabilities had been exploited.

Acknowledgement

Hitachi Energy thanks Nozomi Networks Lab and associates for reporting the vulnerability and working with us to help protecting our customers.

- Dimitri Gasser, Nozomi Networks
- Johannes Willbold, Ruhr-Universität Bochum
- William Blonay
- Flavio Avato

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

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
2023-02-28	1	Initial public release.

DocuSigned by: