REVISION: B
PUBLICATION DATE: 2021-12-07
DOC. IDENTIFIER: 8DBD000061
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Insecure Boot Image Vulnerability in Hitachi Energy Relion® 670/650/SAM600-IO series Products

CVE-2021-35535

Notice

Summary

Hitachi Energy is aware of a report from U.S. Department of Energy CyTRICS researcher of a vulnerability in the Relion 670/650/SAM600-IO series versions listed below. Recommended action for each affected version is listed in the Recommended Immediate Actions Section.

An attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product.

Affected Products and Versions

List of affected products and product versions:

- Relion 670/650 series version 2.2.0 all revisions
- Relion 670/650/SAM600-IO series version 2.2.1 revisions up to 2.2.1.6
- Relion 670 series version 2.2.2 all revisions
- Relion 670 series version 2.2.3 revisions up to 2.2.3.3
- Relion 670/650 series version 2.2.4 all revisions

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-2021-35535 CVSS v3.1 Base Score: 8.1 – High CVSS v3.1 Vector: AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here	A vulnerability exists in the early boot process of the product in which there is a tiny time gap where an older version of VxWorks is loaded prior to booting up the complete application firmware. The older version of VxWorks is a version that is susceptible to Urgent/11 of which successful exploitation allows for remote code execution on the device before operating system is loaded.

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	Refer to Mitigation Factors/Workaround Section or upgrade to version 2.2.5.
* Relion 670/650/SAM600-IO series version 2.2.1 revisions up to 2.2.1.6	Update to revision 2.2.1.7.
* Relion 670 series version 2.2.2 all revisions	Refer to Mitigation Factors/Workaround Section or upgrade to version 2.2.5 or update to Relion 670 series version 2.2.2.5 (planned).
Relion 670 series version 2.2.3 revisions up to 2.2.3.3	Update to revision 2.2.3.4.
* Relion 670/650 series version 2.2.4 all revisions	Refer to Mitigation Factors/Workaround Section or upgrade to version 2.2.5 or update to Relion 670/650 series version 2.2.4.3 (planned).

* Updated in Revision B

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 Relion 670/650 series and SAM600-IO?

Hitachi Energy Relion 670/650 series and SAM600-IO 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.

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could exploit vulnerabilities related to Urgent/11 [1][2].

What might an attacker use the vulnerability to do?

An attacker could hijack existing TCP sessions to inject packets of their choosing or cause Denial-of-Service (DoS) attacks.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by:

1. have a physical access to the device
2. continuously reboot or reconfigure the IED to boot from a remote server
3. connecting to the front Ethernet access port of the device or connected to a local network that the front access port is connected to.

Generally, to make a successful exploitation, an attacker needs at least an access to the system network of which the front access port is connected. This practice is not recommended by Hitachi Energy and can be referred to our security deployment guideline. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access that is connected to the front port of the affected system node could exploit this vulnerability. Recommended practices include that industrial 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. Furthermore, front port of the Relion 670/650/SAM600-IO should not be connected to a network.

When this security advisory was issued, had this vulnerability been publicly disclosed?

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, Hitachi Energy had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

References

1. Security Advisory: WindRiver TCP/IP Stack (IPNet) Vulnerabilities
https://www.windriver.com/themes/Windriver/pdf/security-advisory-ipnet.pdf?v2
2. Urgent/11 – Critical Vulnerabilities to Remotely Compromise VxWorks, the Most Popular RTOS,
https://info.armis.com/rs/645-PDC-047/images/Urgent11%20Technical%20White%20Paper.pdf

Acknowledgement

Hitachi Energy thanks the following for working with us to help protect customers:

U.S. Department of Energy CyTRICS researcher Riley Barello Myers.

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[1] – cybersecurity@hitachienergy.com .

Revision

Date of the Revision	Revision	Description
2021-11-04	A	Initial public release.
2021-12-07	B	Update on Section Recommended Immediate Actions

[1] Signature file of this PDF is available at https://www.hitachienergy.com/cybersecurity/alerts-and-notifications