TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-06-27
DOC. IDENTIFIER: 8DBD000157
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

CYBERSECURITY ADVISORY

OpenSSL Vulnerability in Hitachi Energy's Relion® 670, 650, SAM600-IO series Product

CVE-2022-4304

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 the vulnerability CVE-2022-4304 in the OSS component OpenSSL, that affects the Relion 670, 650, SAM600-IO versions that are listed below. An attacker successfully exploiting this vulnerability could send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. For immediate mitigation/workaround information, please refer to the General Mitigation Factors/Workarounds

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-2022-4304 Detail CVSS v3.1 Base Score: 5.9 MEDIUM CVSS v3.1 Vector:/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Link to NVD: click here	A timing-based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

Recommended Immediate Actions

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

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

CVE Versions	Affected Version	Recommended Actions
CVE-2022-4304	Relion 670/650 series version 2.2.0 all revisions	For all versions apply General Mitigation Factors. Remediation will be available for all affected versions. Update the system once remediated version is available.
	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/SAM600-IO series version 2.2.5 all revisions	

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.

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 pro tection 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?

An attacker who successfully exploits this vulnerability can recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by observing a genuine connection between a client and a server, sending trial messages to the server, and recording the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

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 or could an attacker exploit the vulnerability?

Yes, these vulnerabilities have been publicly disclosed by the respective Open-Source Software.

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.

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
2023-06-27	1	Initial public release.

DocuSigned by:

Issued by: Hitachi Energy

Hitachi Energy

Product Security Incident Response Team