TLP: CLEAR
REVISION: 1
PUBLICATION DATE: 2022-11-15
DOC. IDENTIFIER: 8DBD000120
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Cleartext Credentials Vulnerability on Hitachi Energy's Multiple IED Connectivity Packages (IED ConnPacks) and PCM600 Products

CVE-2022-2513

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of private reports of a vulnerability in multiple IED ConnPacks of the PCM600 versions listed below. An implementation flaw causes credentials of IEDs to be stored in plain text format in the database. Please refer to the Recommended Immediate Actions Section for mitigation strategy.

An attacker who successfully exploited this vulnerability could obtain the IEDs' credentials. With that information, they could gain access to the IEDs, perform unauthorized modifications or provoke a denial-of-service on them.

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-2022-2513 CVSS v3.1 Base Score: 7.1 High CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N Link to NVD: click here CWE-312 – Cleartext Storage of Sensitive Information	A vulnerability exists in the Intelligent Electronic Device (IED) Connectivity Package (ConnPack) credential storage function in Hitachi Energy's PCM600 product included in the versions listed below, where IEDs credentials are stored in a cleartext format in the PCM600 database. An attacker who manages to get access to the exported backup file can exploit the vulnerability and obtain credentials of the IEDs. The credentials may be used to perform unauthorized modifications such as loading incorrect configurations, reboot the IEDs or cause a denial-of-service on the IEDs.

Affected Products and Recommended Immediate Actions

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

Affected Version	Recommended Actions
PCM600 v2.11 and previous versions including Hotfixes[1] (see CPE list in the Appendix) 670 Connectivity Package version from 3.0 to 3.4.1 650 Connectivity Package version from 1.3 to 2.4.1 SAM600-IO Connectivity Package version from 1.0 to 1.2 GMS600 Connectivity Package version from 1.3 to 1.3.1 PWC600 Connectivity Package version from 1.1 to 1.3	Update to PCM600 v2.11 Hotfix 20220923 or apply mitigation factors/workarounds as described in the Mitigation Factors/Workarounds Section.

[1] PCM600 maintains only the latest released version. All previous versions are in obsolete phase in the software life cycle policy and will not be maintained.

Mitigation Factors/Workarounds

It is recommended to implement and continuously revise least privileges principles to minimize permissions and accesses to PCM600 related resources, included the backup file, PCMI/PCMP file. 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.

Additional recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System.

More information to deploy PCM600 securely can be found in the following documents:

1MRS758440, PCM600 Cyber Security Deployment Guideline

Frequently Asked Questions

What is PCM600?

Product PCM600 is a tool that provides versatile functionalities for the entire life cycle of all Relion® protection and control IED applications, at all voltage levels. The tool helps the user to manage the Relion® protection and control equipment all the way from application and communication configuration to disturbance handling, including automatic disturbance reporting

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could obtain the credentials and use it to perform unauthorized modifications or cause a denial-of-service on the IEDs.

How could an attacker exploit the vulnerability?

An attacker needs to have a local access to the PCM600 and explore the database. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

The vulnerability is not bound to a network stack. However, if the PCM600 is setup to access remotely, an attacker does not need to be physically in front of a PCM600 to exploit the vulnerability.

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.

Acknowledgement

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

PSE - Polskie Sieci Elektroenergetyczne (Polish Power Grid Company (PPGC))

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
2022-11-15	1	Initial public release.

DS