REVISION: A
PUBLICATION DATE: 2022-05-10
DOC. IDENTIFIER: 8DBD000080
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

CYBERSECURITY ADVISORY

Multiple Vulnerabilities in Hitachi Energy's TXpert Hub CoreTec 4 Product
CVE-2021-35530
CVE-2021-35531
CVE-2021-35532

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 private report of vulnerabilities in the TXpert Hub CoreTec 4 versions listed below. Remediation and mitigation information is available in the Section Recommended Immediate Actions.

An attacker who successfully exploited those vulnerabilities could cause a denial-of-service to the product, modify configuration, obtain sensitive information from the product and load a malicious firmware.

Affected Products and Versions

List of affected products and product versions:

TXpert Hub CoreTec 4 version 2.0.0, 2.0.1

TXpert Hub CoreTec 4 version 2.1.0, 2.1.1, 2.1.2, 2.1.3

TXpert Hub CoreTec 4 version 2.2.0, 2.2.1

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-2021-35530 CVSS v3.1 Base Score: 6.0 Medium CVSS v3.1 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L Link to NVD: click here	User authentication bypass. A vulnerability exists in the product versions listed above. A flaw in the application authentication and authorization mechanism that depends on a token validation of the session identifier allows an unauthorized modified message to be executed in the server enabling an unauthorized actor to change an existing user password, and further gain authorized access into the system via login mechanism.
CVE-2021-35531 CVSS v3.1 Base Score: 6.0 Medium CVSS v3.1 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L Link to NVD: click here	Remote Code Execution. A vulnerability exists in the product versions listed above. An attacker could exploit the vulnerability by first gaining access to an authorized user with ADMIN or ENGINEER role rights. After that, via a particular configuration setting field the attacker can inject an OS command that is executed by the system.
CVE-2021-35532 CVSS v3.1 Base Score: 6.0 Medium CVSS v3.1 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L Link to NVD: click here	Firmware upload verification bypass. A vulnerability exists in the file upload validation. Exploitation can happen only if an attacker or malicious agent manages to gain access to the system and obtain sufficient permission for firmware update. Afterwards, the attacker can upload a malicious firmware to the product.

Recommended Immediate Actions

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

	CVE-2021-35530 & CVE-2021-35531	CVE-2021-35532
TXpert Hub CoreTec 4 version 2.0.x TXpert Hub CoreTec 4 version 2.1.x TXpert Hub CoreTec 4 version 2.2.x (x: all versions)	Update the system to TXpert Hub CoreTec 4 version 2.3.0 that fixes the issues.	To reduce risk of exploitation, applies mitigation as described in the Section Mitigation Factors/Workarounds.

Hitachi Energy recommends that customers apply the update at the earliest convenience.

Mitigation Factors/Workarounds

Recommended security practices and defense in depth strategy 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 product security deployment guidelines. More information on recommended practices can be found in the following document:

- 1ZBK000069, TXpert Hub CoreTec 4 Software Manual Version 2.x

Hitachi Energy has tested the following workarounds:

- Ensure the users of the system have individual user accounts. No shared user accounts shall be used.
- Users shall only have the minimum rights required.
- All system default users account shall be deleted.

Although these workarounds will not correct the underlying vulnerability, they can reduce the risk of exploitation.

Impact of Workaround

It is important to note that the workaround only increase the level of difficult for an attacker to explore the vulnerability as it requires first that the attacker somehow get on hold of the individual users account information. The attacker must seek for the user accounts with either ADMIN or ENGINEER roles.

Frequently Asked Questions

What is Hitachi Energy TXpert Hub CoreTec 4?

Hitachi Energy TXpert Hub CoreTec 4 is a product which enables real-time management of a transformer by monitoring key health parameters of the transformer and triggering various indicators flags on the web user interface to help the operators to identify any changes in the transformer’s condition.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could cause the affected system node to stop or become inaccessible, also could allow the attacker to take control of the system node.

How could an attacker exploit the vulnerability?

To exploit the user authentication bypass vulnerability, it requires the attacker to first obtain access to the system node network. Then the attacker must enumerate the user accounts identifying the ones with ADMIN or ENGINEER role assignment. With that in place the attacker could craft a message by passing the authentication mechanisms and changing one of these user accounts password. Then the attacker could gain further access to the system by authenticating with the new changed password.

To exploit the Remote Code Execution vulnerability, it requires the attacker to first obtain access to the system node network. Then the attacker must successfully authenticate with any user account assigned either as ADMIN or ENGINEER role. After that, via a particular configuration setting field the attacker can inject an OS command that is executed by the system.

Could the vulnerability be exploited remotely?

No, the vulnerabilities are not bound to a network stack. To exploit the vulnerabilities, an attacker needs to gain access to the affected system node. 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, Hitachi Energy received information internally

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.

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
2022-05-10	A	Initial public release.