REVISION: A
PUBLICATION DATE: 2022-05-10
DOC. IDENTIFIER: 8DBD000081
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Heap-Based Buffer Overflow in Sudo Vulnerability in Hitachi Energy's TXpert Hub CoreTec 4 Product

CVE-2021-3156

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a report of Heap-Based Buffer Overflow in Sudo (Baron Samedit) that affects most Linux-based Operating Systems of which is the Operating System used in the TXpert Hub CoreTec 4 versions listed below. An update is available that resolves the vulnerability.

An attacker who successfully exploited the vulnerability could allow unauthorized privilege escalation to root account.

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.

Sudo Baron Samedit

Vulnerability ID	Detail Description
CVE-2021-3156 CVSS v3.1 Base Score: 7.8 High CVSS v3.1 Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	Sudo is included in most of Linux operating system, including the one that is used in TXpert Hub CoreTec 4. Sudo before version 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character

Recommended Immediate Actions

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

Affected Version	Recommended Actions
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.

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 mitigation:

- Remove Secure Remote Access (SSH) as described in the System Hardening section of the Security Deployment Guidelines. This will not remove the vulnerable component but it will remove the ability to remote access the command line interface and exploit the vulnerability.

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 take control of the system node.

How could an attacker exploit the vulnerability?

To exploit this vulnerability. It requires the attacker to first obtain access to TXpert Hub CoreTec 4 command line interface which can be done via SSH protocol when the service is enabled. An attacker would also have to successfully authenticate into the command line with an existing user credentials prior to exploit the Sudo vulnerability.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node and successfully authenticate to SSH could exploit this vulnerability. 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?

Yes, the vulnerabilities related to the Open-Source Software have been publicly disclosed by the respective Open-Source community.

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

While an exploit to the CVE-2021-3156 Linux x64 is available [1] Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

References

1. https://github.com/worawit/CVE-2021-3156

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.