REVISION: A
PUBLICATION DATE: 2021-11-23
DOC. IDENTIFIER: 8DBD000069
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Ports Vulnerabilities in Hitachi Energy XMC20 Product

CVE-2021-40333
CVE-2021-40334

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of private reports of vulnerabilities in the XMC20 versions listed below. Recommended action for each affected version is listed in the Recommended Immediate Actions Section.

An attacker who successfully exploited these vulnerabilities, could gain unauthorized access to the Data Communication Network (DCN) routing configuration and cause a disruption to the Network Management System (NMS) and Network Element (NE) communication.

Affected Products and Versions

List of affected products and product versions:

- XMC20 product version earlier than R15A.

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, wh1ich 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-2021-40333 CVSS v3.1 Base Score: 9.0 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H Link to NVD: click here	The vulnerability is a weak default credential associated with TCP port 26. Successful exploitation of this vulnerability allows attacker to gain unauthorized access to the Data Communication Network (DCN) routing configuration.
CVE-2021-40334 CVSS v3.1 Base Score: 8.6 High CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Link to NVD: click here	The vulnerability is due to the implementation of the proprietary management protocol (port TCP 5558) in which if SSH is activated, it can cause a disruption to the NMS and NE communication.

Recommended Immediate Actions

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

Affected Version	Recommended Actions for Each CVE-ID	
	CVE-2021-40333 *Affect only CENT2*	**CVE-2021-40334**
XMC20 version earlier than R15A	• Fixed in XMC20 R14A Hotfix ○ CENT2 – cent2_r2a16_03 or newer	• For XMC20 version R14A, please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy

	• Fixed in XMC20 version R15A,
	  ○ CENT2 – cent2_r15a06 or newer
		• Fixed in XMC20 version R15A
		  ○ CENT2 – cent2_r15a06 or newer
		  ○ CO5NE – co5ne_r1506 or newer
		  ○ CO5UN – co5un_r1506 or newer

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

Mitigation Factors/Workarounds

Recommended security practices and firewall configurations help protecting systems from attacks that originate from outside the network. Such practices include that network management systems and XMC20 networks are typically physically protected from direct access by unauthorized personnel and have no direct connections to the Internet, as well as are separated from other networks by means of a firewall system that has a minimal number of ports exposed (e.g., traffic to TCP port 26 should be blocked/dropped), and others that have to be evaluated case by case. 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 XMC20 Product?

The XMC20 is a network element that can be used either as multiservice access system for point of presence applications or as a network element carrying out networking functions (e.g., digital cross-connect, gateway, channel bank).

The XMC20 network element includes a packet-based core and a circuit-based core. Protocol conversion functions allow the transport of Ethernet frames over PDH or SDH.

What is the scope of the vulnerability?

The vulnerability affects the XMC20, however when exploited, the vulnerability may cause a disruption to the NMS and NE communication.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the CVE-2021-40333 vulnerability (related to TCP port 26), could gain unauthorized access to the DCN routing configuration and change the DCN routing without customer knowledge.

As for the CVE-2021-40334 vulnerability (related to TCP port 5558), successful exploitation may disrupt the NMS/NE communication.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node 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?

No, this vulnerability has not been publicly disclosed, Hitachi Energy received information about this vulnerability 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 these vulnerabilities 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[1] – cybersecurity@hitachienergy.com .

Revision

Date of the Revision	Revision	Description
2021-11-23	A	Initial public release.

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