TLP:CLEAR

REVISION: 2
PUBLICATION DATE: 2022-12-22
DOC. IDENTIFIER: 8DBD000084
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Vulnerabilities in Hitachi Energy's UNEM Product

CVE-2021-40341
CVE-2021-40342
CVE-2022-3927
CVE-2022-3928
CVE-2022-3929

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the use of Data Encryption Standard (DES) algorithm in the UNEM and as well on multiple hardcoded credentials and non-secure communication used in the UNEM. For details, please refer to the Vulnerability ID, Severity and Details section. An attacker that manages to exploit these vulnerabilities, may obtain sensitive information and gain access to the network elements that are managed by the UNEM and could also cause availability issue on the UNEM.

Please find remediation and mitigation information in the section Affected Products and Recommended Immediate Actions.

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 analyse the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2021-40341 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-326 – Weak encryption strength	UNEM utilizes the DES cypher to encrypt user credentials used to access the Network Elements. DES is no longer considered secure because it uses a 56-bit key that is too short, allowing the cypher to be decrypted in a short time.
CVE-2021-40342 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-326 – Weak encryption strength	UNEM's DES implementation uses a default key for encryption. An attacker that manages to exploit this vulnerability will be able to obtain sensitive information and gain access to the network elements that are managed by the UNEM.
CVE-2022-3927 CVSS v3.1 Base Score: 8.0 High CVSS v3.1 Vector: AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here CWE-321 – Use of Hard-coded Cryptographic Key	Public and private key are found in UNEM used to sign and protect Custom Parameter Set (CPS) file from modification. An attacker that manages to exploit this vulnerability will be able to change the CPS file, sign it so that it is trusted as the legitimate CPS file.
CVE-2022-3928 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-321 – Use of Hard-coded Cryptographic Key	Hardcoded credential is found in UNEM message queue. An attacker that manages to exploit this vulnerability will be able to access data to the internal message queue.
CVE-2022-3929 CVSS v3.1 Base Score: 8.3 High CVSS v3.1 Vector: AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here CWE-319 – Cleartext Transmission of Sensitive Information	Communication between the client (UNEM User Interface) and the server application (UNEM Core) is partially using CORBA (Common Object Request Broker Architecture) over TCP/IP. This protocol is not encrypted and allows to trace internal messages.

Affected Products and Recommended Immediate Actions

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

CVEs	Affected Version	Recommended Actions
CVE-2022-3928 CVE-2022-3929	UNEM R15B	The vulnerabilities are remediated in UNEM R16A.
	UNEM R15A*	Please upgrade to UNEM R16A.
	UNEM R14B* UNEM R14A* UNEM R11B* UNEM R11A* UNEM R10C* UNEM R9C* Included all subversions*	For immediate recommended mitigation action if using UNEM R15B and earlier, please refer to the following clause of section Mitigation Factors/Workarounds in this document: - Secure the NMS CLIENT/SERVER communication.
CVE-2022-3927	UNEM R15B	The vulnerabilities are remediated in UNEM R16A.
	UNEM R15A*	Please upgrade to UNEM R16A.
	UNEM R14B* UNEM R14A* UNEM R11B* UNEM R11A* UNEM R10C* UNEM R9C* Included all subversions*	For immediate recommended mitigation action if using UNEM R15B and earlier, follow the recommended security practices as described in section Mitigation Factors/Workarounds in this document.
CVE-2021-40341 CVE-2021-40342	UNEM R16A	The vulnerabilities are partially remediated in UNEM R16A, the full remediation will be done in the upcoming UNEM release (planned).
	UNEM R15B UNEM R15A* UNEM R14B* UNEM R14A* UNEM R11B* UNEM R11A* UNEM R10C* UNEM R9C* Included all subversions*	For immediate recommended mitigation actions if using UNEM R16A and earlier, please refer to the following clause of section Mitigation Factors/Workarounds in this document: - Database contains credentials with weak encryption. For immediate recommended mitigation actions if using UNEM R15B and earlier, please refer to the following clause of section Mitigation Factors/Workarounds in this document: - Secure the NMS CLIENT/SERVER communication. - Embedded ECST with RADIUS authentication should be avoided. - Database contains credentials with weak encryption.

*** No maintenance activity on this version.**

Mitigation Factors/Workarounds

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. Additionally, ensure that only authorized personnel(s) have access to the system configuration file.

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.

Specific mitigation factors:

1. *Secure the NMS CLIENT/SERVER communication*. To secure the NMS Client/Server communication, follow the guideline “1KHW029191-UNEM Client - Server Setup in a Secure Network”.
2. *Embedded ECST with RADIUS authentication should be avoided*. Problem exists only when remote authentication to Network Elements (NE) is used, alternatively from UNEM R14A onwards it is possible to generate and exchange private/public keys, creating a trusted relation between UNEM and XMC20 network elements.
3. *Database contains credentials with weak encryption*. It is important to ensure that the exported files shall be handled in secure way to ensure that only authorized persons can access them. To protect the database backup files, user access control or encrypting are possible solutions.

Frequently Asked Questions

What is UNEM?

UNEM is one of the elements in Hitachi Energy's comprehensive Network Management System (NMS) suite, is a powerful toolset providing all the essentials of a Network Management System, such as network status, alarm notification, and enhanced circuit provisioning functionality.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the vulnerability could take control of the Network Elements managed by the UNEM system.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by breaking the DES cipher using a brute force attack. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigation Factors/Workarounds above.

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 yet been publicly disclosed before.

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:
K-Businesscom AG, Austria

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
2022-12-13	1	Initial public release.
2022-12-22	2	Added acknowledgement to K-Businesscom AG, Austria

DS