REVISION: E
PUBLICATION DATE: 2022-01-05
DOC. IDENTIFIER: 8DBD000089
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy's UNEM Product

CVE-2021-44228
CVE-2021-45046
CVE-2021-45105

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the vulnerabilities [1] – CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 in Apache Log4j v2.x that are used in the product versions listed below. The product versions listed in this document are affected only by the Apache Log4j v2.x vulnerabilities as elaborated in the Section Vulnerability ID, Severity and Details.

For immediate mitigation/workaround information, please refer to the Mitigation Factors/Workaround Section below.

Affected Products and Versions

List of affected products and product versions:

– UNEM R15A

– UNEM R14B

– UNEM R14A

– UNEM R11B

– UNEM R11A

– UNEM R10 series

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-2021-44228 CVSS v3.1 Base Score: 10 CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here	An exploitable remote code execution vulnerability exists in the Apache Log4j versions between 2.0 and 2.14.1. The present vulnerability impacts the UNEM product, by permitting the attacker to send a specially crafted message, that may result in loading an external code class or message lookup and the execution of that code in a vulnerable targeted server over a network.
CVE-2021-45046 CVSS v3.1 Base Score: 9.0 CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments.

CVE-2021-40105 CVSS v3.1 Base Score: 7.5 CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here	Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial-of-service when a crafted string is interpreted.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
UNEM versions R15A, R14B, R14A, R11B SP1, R11A, R11A SP1	A patch is available for releases R15A, R14B, R14A, R11B (incl. SP1) and R11A (incl. SP1). For details on how to apply such patch, please refer to the technical bulletin "*UNEM - Installation of Log4j Patch*", version B (1KHW029176) available in the Hitachi Energy Customer Connect Portal.
UNEM versions versions R11A and R10 series	Apply General Mitigations and upgrade to latest version. For upgrades, please get in touch with your Hitachi Energy contacts.

General Mitigation Factors/Workarounds

The Purdue Enterprise Reference Architecture model should be followed, where recommended security practices and firewall configurations can help protecting a process control network from attacks that are originated from outside the network. Such practices include that process control systems are 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.

Frequently Asked Questions

What is Hitachi Energy UNEM product?

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 this vulnerability, can insert and run arbitrary code on the targeted system.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability, by creating a specially crafted message and sending the message to an affected process. This would require that the attacker has access to the system network.

Recommended practices help to mitigate such attacks, see section Mitigating Factors 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 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 Apache Log4j vulnerability has been disclosed.

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

While instances of exploits to the Apache Log4j vulnerability have been reported, Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

References

1. Apache Log4j Security Vulnerabilities - https://logging.apache.org/log4j/2.x/security.html

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
2021-12-15	A	Initial public release.
2021-12-21	B	Add additional relevant CVE-2021-45046
2021-12-22	C	Add additional relevant CVE-2021-45105 Patch information is available in Recommended Immediate Action Section
2021-12-23	D	Added information concerning R11A
2022-01-05	E	Updated Recommended Immediate Actions • Added information concerning patching of R11A series