REVISION: B
PUBLICATION DATE: 2021-12-21
DOC. IDENTIFIER: 8DBD000095
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy's Lumada Enterprise Asset Manager & Field Service Manager (EAM-FSM) Product

CVE-2021-44228
CVE-2021-45046

Notice

Hitachi Energy

Summary

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

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

Hitachi Energy will continue to investigate and update this advisory as more information becomes available.

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: 10.0 CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L Link to NVD: click here	In the affected version of Apache Log4j, JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.
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.

Recommended Immediate Actions

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

Affected Application	Application Versions	Recommended Actions
Lumada EAM / FSM	v1.7.x, v1.8.x, v1.9.x	See Section Mitigation Strategy below
3rd party – Elastic Search [2] - Kibana	Elasticsearch versions 5.0.0+	Set the JVM option `-Dlog4j2.formatMsgNoLookups=true` and restart each node of the cluster.

Mitigation Strategy

A. Log4j vulnerability mitigation - Lumada EAM and FSM

1. For log4j versions < 2.10 this behavior can be mitigated by removing the JNDILookup class from the classpath.
2. Configure Kubernetes to send the Java JVM property `-Dlog4j2.formatMsgNoLookups=true` to all pods [3] (or the equivalent environment variable, LOG4J_FORMAT_MSG_NO_LOOKUPS). https://stackoverflow.com/questions/54550933/kubernetes-shared-environment-variables-for-all-pods
3. Configure HAPROXY to reject questionable requests and run tests to confirm remediation / mitigation is successful [4]. https://www.haproxy.com/blog/december-2021-log4shell-mitigation/
4. Accept and upgrade Lumada EAM/FSM to the latest patched version for 1.7.x, 1.8.x, and 1.9.x. All Java-based services in use by Lumada EAM and FSM have been upgraded to use log4j version 2.16.0 to address both vulnerabilities that have been identified.

B. Open Distribution Elastic Search

1. Login as root users or super user
2. Edit /etc/elasticsearch/jvm.options
3. Add the following lines:

```
##Log4j Vulnerability Update
-Dlog4j2.formatMsgNoLookups=true
```

4. Restart each ElasticSearch Node

General 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.

Frequently Asked Questions

What is the Hitachi Energy Lumada EAM / FSM product?

Lumada EAM software combines proven practices in enterprise asset management (EAM) across a range of sectors including utilities, mining, oil and gas, enabling peak operational performance and continuous process improvement. Built specifically to support the complete lifecycle of complex, critical and costly assets, the Lumada EAM system includes complete enterprise functionality across asset management and maintenance, scheduling and execution, work planning, supply chain and material planning, multi-entity financial, and people management.

Lumada FSM enterprise field service management (FSM) solution is designed to enhance efficiency, productivity and safety. The Lumada FSM system is a cloud-based solution that equips mobile users to execute

work orders in the field safely and efficiently. The solution is designed specifically to extend the efficiency of the enterprise asset management process directly to the supporting assets, and drive fieldwork productivity and worker safety.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can insert and run arbitrary code on the EAM / FSM server.

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, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that the attacker installs malicious software on a system node or otherwise infects the network with malicious software.

Recommended practices help 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 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 Apache Log4j vulnerability has been disclosed.

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

Hitachi Energy has observed different reports that the Apache Log4j vulnerability is being exploited in the wild.

References

1. Apache Log4j Security Vulnerabilities - https://logging.apache.org/log4j/2.x/security.html
2. Elastic Search - https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
3. Configuring Kubernetes shared environment variables for all Pods - https://stackoverflow.com/questions/54550933/kubernetes-shared-environment-variables-for-all-pods
4. HAProxy log4shell mitigation - https://www.haproxy.com/blog/december-2021-log4shell-mitigation/

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