REVISION: C
PUBLICATION DATE: 2022-01-12
DOC. IDENTIFIER: 8DBD000087
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy's Lumada Asset Performance Management (APM) Product

CVE-2021-44228

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Hitachi Energy or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Hitachi Energy or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Hitachi Energy and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Summary

Hitachi Energy is aware of the vulnerability – CVE-2021-44228, [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 vulnerability 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.

Affected Products and Versions

List of affected products and product versions:

- Lumada APM Software-as-a-Service (SaaS) offering
- Lumada APM On-premises versions 5.0 and later.

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:C/C:H/I:H/A:H/E:U/RL:O/RC:R 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 injecting malicious commands. As it is used in the prognostic model execution service of Lumada APM and Epiphany platform, an attacker who can open connections to Lumada APM services or platform can potentially execute arbitrary code within the application or its platform.

Note that we removed CVE-2021-45056 from the list of vulnerability as our investigation concluded that Lumada APM is not affected by the CVE-2021-45056.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Lumada APM SaaS	No action is required by customers. Hitachi Energy has remediated the aforementioned vulnerability in the Hitachi Energy managed SaaS environments.
Lumada APM On-premises	Hitachi Energy delivers the Lumada APM application to customers. However, in order for the Lumada APM application to run, it also needs Epiphany platform, which is a 3rd party Open-Source Software. In this advisory, we elaborate how Lumada APM application is affected by the vulnerability and provide the mitigation and remediation information. In addition, we also provide information related to Epiphany and a way to help customer obtain the Apache Log4j v2.17.1 for Epiphany. This advisory does not elaborate how Epiphany is affected by the Apache Log4Shell vulnerabilities. Please apply the following actions: • Lumada APM services remediation actions (depending on version see “Lumada APM services actions” below) or mitigation factors • Epiphany platform actions (see “Epiphany platform actions” below)

Lumada APM Services Remediation Actions

The following remediations are available for Lumada APM Services.

Lumada APM On-premises versions	Recommended Actions
5.0 or later	None (Lumada APM services are not affected in this case)
6.0.0.0, 6.0.0.1 or 6.0.0.2	Upgrade to version 6.3.0.1 (available) or apply the version 6.0.0.3 patch (planned).
6.1.0.0	Update to version 6.1.0.1 patch (available) or upgrade to version 6.3.0.1 (available).
6.2.0.0 or 6.2.0.1	Update to at least version 6.2.0.2 patch (available) or upgrade to version 6.3.0.1 (available)
6.3.0.0	Update to at least version 6.3.0.1 (available).

Note: for all available patches except for Lumada APM version 6.3.0.1, the Apache Log4j v2.17 has been integrated even though Lumada APM is affected only by CVE-2021-44228. Lumada APM version 6.3.0.1 integrates the Apache Log4j v2.15.0 that remediates the CVE-2021-44228.

Lumada APM Services Mitigation Factors

The vulnerability of the Apache Log4j – CVE-2021-44228 on Lumada APM application services is limited to the *Prognostic model execution service* (“apm-prognostic-model-executor" or “apm-prognostic-model-executor-arm64" for ARM64 platform) only. The service is used when prognostic performance models are executed. To mitigate the vulnerability without applying an upgrade or a patch to affected versions of Lumada APM services,

the *Prognostic model execution service* should be disabled. (Refer to the Lumada APM documentation on how to scale the service to zero instances).

Epiphany Platform Recommended Actions

Lumada APM services rely on Epiphany platform and one of the standard components of Epiphany is Open Distro for Elasticsearch. The recommended action to address the vulnerability is to apply configuration changes and update Log4j library versions used in OpenDistro to Apache Log4j version 2.17.1 (that remediates the CVE-2021-44228, CVE-2021-45056, CVE-2021-45105 and CVE-2021-44832) using provided script package **EpiphanyPatch_OpenDistro_log4J**. The configuration change is one of the following :

- If the logging server has the `/etc/elasticsearch/jvm.options.d/` catalog, create there the `nolog4j0day.options` file that has this setting: `-Dlog4j2.formatMsgNoLookups=true`
- If there is no such catalog, open the `/etc/default/elasticsearch` file and add this line: `ES_JAVA_OPTS="-Dlog4j2.formatMsgNoLookups=true"`

When the above changes are applied, use the provided script to update the Log4j libraries, which should also restart the service. Refer to the documentation available with the script on how to properly execute it.

To restart the service manually you can use this command:

```
sudo systemctl restart elasticsearch.service
```

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 Lumada Asset Performance Management (APM)?

Lumada APM is a solution for enterprise level customers (not mass market) allowing centralized, high-level analytics of assets fleet condition. It is a web-based solution offered both as a cloud-based service (Software-as-a-Service), as well as an “on premises” variant. It is deployed on Epiphany platform – a unified set of software components for microservice oriented applications.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability in Lumada APM services could potentially be able to insert and run arbitrary code on the prognostic model execution service, stop it or make it inaccessible, use it to communicate to other internal Lumada APM services and other parts of the virtual or physical network APM resides in, which could also lead to exposing the data APM processes and has access to.

An attacker who successfully exploited this vulnerability in Epiphany platform could potentially be able to insert and run arbitrary code on the machines hosting the application, stop them or make inaccessible, including

communication to Lumada APM application services and other parts of the virtual or physical network APM resides in, which could also lead to exposing the data APM processes have access to.

How could an attacker exploit the vulnerability?

To exploit the vulnerability in Lumada APM application services, the attacker could provide malicious data for assets monitored in APM which use one of the prognostic models. This would require authenticated access to APM's user interface or APM's integration API-s. Limiting access to APM and disabling the prognostic model execution service would help to mitigate such attacks. See section Mitigating Factors above.

To exploit the vulnerability in Epiphany platform, the attacker could provide malicious information by sending a specially crafted request to one of exposed network interfaces (e.g., the APM's exposed HTTP services). This would require access to platform's network external interfaces. Limiting network access, utilizing web application firewalls and similar network security practices would help to mitigate such attacks. See sections for recommended actions for Epiphany platform, Mitigating Factors and General Mitigation Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to affected system nodes 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, although its full relevance to Lumada APM was not.

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. There was no report on it being exploited in Lumada APM installations.

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
2021-12-17	A	Initial public release.
2021-12-21	B	Added additional relevant CVE-2021-45046
2022-01-12	C	Removed CVE-2021-45046 as our investigation revealed that Lumada APM is not affected by the vulnerability. Updated Lumada APM patch availability. Updated the Epiphany Platform Actions.