REVISION: D
PUBLICATION DATE: 2021-12-22
DOC. IDENTIFIER: 8DBD000091
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy's Network Manager Advanced Distributed Management System (NM-ADMS) Product

CVE-2021-44228
CVE-2021-45046

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the Apache Log4j 2.x vulnerability [1] – CVE-2021-44228 that is used in the Network Manager product versions listed in the Recommended Immediate Action Section. The product versions listed in this document are affected only by the Apache Log4j 2.x vulnerabilities as elaborated in the Section Vulnerability ID, Severity and Details.

An attacker who successfully exploits this vulnerability could perform unauthenticated remote code execution on the affected product.

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:C/C:H/I:H/A:H 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
Network Manager Outage Management Interface (OMI) – Client Application	9.0 – 9.1.0.44**	Follow instructions for Windows applications in section A.1**.
	9.1.1	Follow instructions for Windows applications in section A.1**.
	10.3.4	Follow instructions for Windows applications in section A.1**.
Network Manager ADMS Network Model Server	9.1.0.32 – 9.1.0.44	Follow instructions for Linux applications in section A.2**.
* Third Party – Oracle Database Components - Trace File Analyzer - SQL Developer - Property Graph	12.1, 12.2, 19c	**Note**: Oracle database [2] itself is not affected by this vulnerability. While the components listed are not required by the NM-DMS product, they must not be used until patched to avoid any possibility of exploit. As this is a third-party component, a separate patch management report will be provided to customers with the steps to apply the Oracle provided patches for these components.

* Updated in Revision B. ** Updated in Revision D.

Mitigation Factors

A. Log4j versions 2.x

For log4j versions 2.x this behavior can be mitigated by removing the JNDILookup class from the classpath.

A.1. Windows Applications

Pre-req:

- To perform these steps a zip application must be installed on each Windows instance – examples are Winzip or 7zip.

Steps:

1. Navigate to the client installation lib directory
2. Locate the file with name log4j-core-2.x.x.jar
   a. Note: the JNDI Lookup class only exists in the log4j-core file, log4j-api does not need any modification.
3. Run the following command (substitute the exact file name)

```
zip -q -d log4j-core-2.x.x.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

4. To verify that the command is successful, run the command again and you should see following error:

```
zip error: Nothing to do! (log4j-core-2.x.x.jar)
```

5. Restart Client Applications

A.2. Linux Applications

Pre-req:

- To perform these steps a zip application must be installed on each Linux instance – example is zip binary provided by RHEL.

Steps:

1. Navigate to the application installation directory:

   ```
   cd $CADOPS_HOME/java/dist/lib
   ```

2. Locate the file with name log4j-core-2.x.x.jar
   a. Note: the JNDI Lookup class only exists in the log4j-core file, log4j-api does not need any modification.
3. Run the following command (substitute the exact file name)

   ```
   zip -q -d log4j-core-2.x.x.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
   ```

4. To verify that the command is successful, run the command again and you should see following error:

   ```
   zip error: Nothing to do! (log4j-core-2.x.x.jar) .
   ```

5. Restart Server Applications

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 NM-ADMS product?

Network Manager ADMS is a distribution operations platform that comprises Outage Management System (OMS), Network Applications (NA), Distributed Energy Resource Management System (DERMS), Mobility and Distribution Analytics.

It provides operators with the situational awareness and software tools to reduce the impact of power outages and improve reliability and system efficiency, resulting in improved reliability indices and greater customer satisfaction.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can insert and run arbitrary code on the Network Manager DMS 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 (CVE-2021-44228) is being exploited in the wild, however we are not aware that our products are targeted by the exploit.

References

1. Apache Log4j Security Vulnerabilities - https://logging.apache.org/log4j/2.x/security.html
2. Oracle Security Alert Advisory - https://www.oracle.com/security-alerts/alert-cve-2021-44228.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
2021-12-16	A	Initial public release.
2021-12-20	B	Update in Section Recommended Immediate Actions • Third party – Oracle Database Components
2021-12-21	C	Add additional relevant CVE-2021-45046
2021-12-22	D	Update in Section Recommended Immediate Actions • Removed references to versions < or > 2.10 as all mitigation steps now apply to 2.x. Update in Section Mitigation Factors • Now only a single section regardless of log4j version that explains steps for Windows or Linux Applications. Added pre-req of requiring zip application with examples.