CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy's Network Manager SCADA/EMS, Ranger and NMR Products
CVE-2021-44228
CVE-2021-45046

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 vulnerabilities – CVE-2021-44228 and CVE-2021-45046 [1] in the Apache Log4j v2.x component that are part of Oracle Database's components which are delivered together with the Hitachi Energy's Network Manager SCADA/EMS, Ranger and NMR products. The Network Manager SCADA/EMS, Ranger and NMR products use the Oracle infrastructure but the Network Manager application itself is not vulnerable to CVE-2021-44228 and CVE-2021-45046.

The Oracle database components listed in this document are delivered as part of Hitachi Energy's Network Manager SCADA/EMS, Ranger and NMR products and consequently, are affected by the vulnerabilities related to the Apache Log4j v2.x as elaborated in the Section Vulnerability ID, Severity and Details. Please refer to the recommended immediate actions for remediation/mitigation strategy.

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
Third Party – Oracle Database Components - Trace File Analyzer - SQL Developer - Property Graph	12.1, 12.2, 19c	**Note**: Oracle database contains these three components, trace file analyzer, SQL developer and property graph, and these three components are vulnerable to the CVE-2021-44228 and CVE-2021-45046. [2]. While the components listed are not required by the NM-SCADA/EMS, Ranger and NMR product, they must not be used until patched to avoid any possibility of exploit. As these are third-party components, a separate patch management report 1KPG000001D1968 - Patch Management Oracle advisory for log4j has been made available where the NM-SCADA/EMS, Ranger and NMR are tested against the Oracle's patches for these components. In the future, please refer to the released patch validation report. For customers with a self-installed/managed Oracle instance it is recommended that you check frequently the Oracle advisory page for any updates and patches - Oracle Security Alert Advisory - https://www.oracle.com/security-alerts/alert-cve-2021-44228.html For customers that desire assistance with the application of Oracle's recommended patch plan they should not hesitate to reach out to their Hitachi Energy customer/client service representative.

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 are the Hitachi Energy NM-SCADA/EMS, Ranger and NMR products?

The Network Manager SCADA/EMS, Ranger and NMR solution helps utilities, transportation, and industrial customers to efficiently control and manage their electric power and pipeline networks for improved reliability and optimal performance.

What might an attacker use the vulnerability to do?

An attacker who exploits the vulnerabilities can control log messages or log message parameters and can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

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. Oracle has also issued its security alert advisory [2].

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. 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
2021-12-17	A	Initial public release.
2021-12-20	B	Updated Section Recommended Immediate Actions • Third party – Oracle Database Components
2021-12-21	C	Added additional relevant CVE-2021-45046
2021-12-21	D	Added Ranger and NMR as affected product family.
2021-12-28	E	Updated Section Recommended Immediate Actions • Added Oracle Security Alert Advisory
2022-01-26	F	Updated Summary Section to make clear that NM SCADA/EMS, Ranger or NMR are not affected. But the Oracle components as part of deliverables are. Updated Section Recommended Immediate Actions • Added patch validation report