REVISION: H
PUBLICATION DATE: 2021-12-29
DOC. IDENTIFIER: 8DBD003132
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY NOTIFICATION

Apache Log4j Vulnerabilities

CVE-2019-17571
CVE-2021-4104
CVE-2021-44228
CVE-2021-44832
CVE-2021-45046
CVE-2021-45105

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.

© Copyright 2021 Hitachi Energy. All rights reserved.

Hitachi Energy

Summary

Hitachi Energy is aware of the Apache Log4j v2.x vulnerabilities called Log4Shell CVE-2021-44228 and CVE-2021-45046 that are published on 2021-12-10 and 2021-12-13 respectively. Another vulnerability CVE-2021-45105 and CVE-2021-44832 applicable to Apache Log4j 2.x is published on 2021-12-16 and 2021-12-28 respectively. As published [1], if the vulnerabilities are exploited, an attacker may launch a remote code execution attack to take control of an affected system and for the CVE-2021-45105 vulnerability, it can cause a denial-of-service if exploited.

Hitachi Energy is also aware of the Apache Log4j 1.x. vulnerabilities CVE-2019-17571 and CVE-2021-4104. If the vulnerabilities are exploited, this allows a remote attacker to execute code on the server.

Apache Log4j v2.x Product Related Advisories

We have completed the investigation of our products from our portfolio related to Apache Log4j v2.x vulnerabilities, specifically CVE-2021-44228 and CVE-2021-45046. To date, the known affected products related to those vulnerabilities are listed below, and if the product is not listed, it is not vulnerable to the aforementioned vulnerabilities. Some of the products' advisories here have also addressed the vulnerability CVE-2021-45105. Please refer to each individual product advisory for more details.

- Axis
- Counterparty Settlement & Billing (CSB) version 6
- e-Mesh™ Monitor
- FOXMAN-UN
- Lumada Asset Performance Management
- Lumada Enterprise Asset Management
- Lumada Field Service Management
- MMS product – Internal Facing Subcomponents
- Network Manager Advanced Distributed Management Systems
- Network Manager SCADA/EMS, Ranger and NMR
- nMarket Global I-SEM
- RelCare
- UNEM

Apache Log4j v1.x Product Related Advisories

To date, the known affected products related to Apache Log4j v1.x vulnerabilities are listed in the list here. Hitachi Energy is continuing to evaluate if any of our products and cloud offerings are affected by those vulnerabilities. Should there be an affected product, the link to the respective advisory will be made available in the list and on our Cybersecurity Alerts and Notifications page.

- nMarket Global I-SEM
- nMarket
- nMarket Global

© Copyright 2021 Hitachi Energy. All rights reserved.

Other Apache Log4j v2.x Vulnerabilities

We understand that there are additional vulnerabilities affecting Apache Log4j v2.x, i.e. CVE-2021-45105 and CVE-2021-44832. Hitachi Energy is continuing to evaluate if any of our products and cloud offerings are affected by those vulnerabilities. Should there be an affected product, we will publish an advisory in our Cybersecurity Alerts and Notifications page. We will handle these two vulnerabilities and any upcoming Apache Log4j vulnerabilities according to our published Software vulnerability handling policy.

General Mitigation Factors

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.

Support

For additional information and support please contact your product provider or Hitachi Energy's service organization. See https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

References

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

Revision

Date of the Revision	Revision	Description
2021-12-13	A	Initial public release.
2021-12-15	B	Added product FOXMAN-UN and UNEM
2021-12-16	C	Added product NM-ADMS, CSB, Lumada EAM, Lumada FSM
2021-12-17	D	Added Axis, NM-SCADA/EMS, nMarket Global I-SEM, Lumada APM, MMS Internal Facing Subcomponent
2021-12-20	E	Added RelCare product Update Summary section and add Other Apache Log4j Vulnerabilities Section
2021-12-22	F	Added e-Mesh™ Monitor product

© Copyright 2021 Hitachi Energy. All rights reserved.

		Added Ranger and NMR as part of Network Manager SCADA/EMS product family
2021-12-23	G	Restructure the Cybersecurity Notification Added affected products related to Apache Log4j v1.x vulnerabilities
2021-12-29	H	Added information related to CVE-2021-44832

© Copyright 2021 Hitachi Energy. All rights reserved.