REVISION: A
PUBLICATION DATE: 2021-12-23
DOC. IDENTIFIER: 8DBD000099
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Apache Log4j v1.x Vulnerabilities in Hitachi Energy's nMarket Product

CVE-2019-17571
CVE-2021-4104

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the Apache Log4j v1.x vulnerabilities [1] – CVE-2019-17571 and CVE-2021-4104 that are used in the product versions listed below. An attacker who successfully exploited this vulnerability could perform unauthenticated remote code execution on the affected product. The product versions listed in this document are affected only by the Apache Log4j v1.x vulnerabilities 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:

– nMarket NY – 4.1.45 and prior

– nMarket NE – 4.6.26 and prior

– nMarket PJM – 5.4.28 and prior

– nMarket TX – 3.1.18 and prior

– nMarket CAISO – 2.9.30 and prior

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-2019-17571 CVSS v3.1 Base Score: 9.8 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	In the affected version of Apache Log4j v1.x, there exist a flaw in a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data.
CVE-2021-4104 CVSS v3.1 Base Score: 8.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	In the affected version of Apache Log4j, the JMSAppender is vulnerable to deserialization of untrusted data when the attacker has written access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
nMarket NY – 4.1.45 and prior nMarket NE – 4.6.26 and prior nMarket PJM – 5.4.28 and prior nMarket TX – 3.1.18 and prior nMarket CAISO – 2.9.30 and prior	Please follow the General Mitigation Factors/Workarounds described below. Please be advised that Hitachi Energy is planning a software release for March 2022 or sooner. Please plan to deploy this release once available.

General Mitigation Factors/Workaround

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 Hitachi Energy's nMarket Product?

nMarket is a software solution for automated trading, communication and settlements with wholesale power markets.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can insert and run arbitrary code on the application.

How could an attacker exploit the vulnerability?

For an attacker to exploit the vulnerability the JMSAppender has to be configured in Apache Log4j 1.x used in the application. An attacker could try to exploit the vulnerability by sending a send malicious serialized data from a malicious server to Log4j open port on victim server. 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 vulnerabilities have been disclosed.

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

While instances of exploits to the Apache Log4j vulnerability have been reported, Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

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
2021-12-23	A	Initial public release.