CYBERSECURITY ADVISORY

Apache Log4j v2.x Vulnerabilities in Hitachi Energy’s Counterparty Settlement and Billing (CSB) Product
CVE-2021-44228
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.
Summary

Hitachi Energy is aware of the vulnerabilities [1] – CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 in Apache Log4j v2.x that are used in the product versions listed below. The product versions listed in this document are affected only by the Apache Log4j v2.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.

Affected Products and Versions

List of affected products and product versions:
- Counterparty Settlement and Billing (CSB) version 6

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.

<table>
<thead>
<tr>
<th>Vulnerability ID</th>
<th>Detail Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2021-44228</td>
<td>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.</td>
</tr>
<tr>
<td>CVE-2021-45046</td>
<td>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 allow 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.</td>
</tr>
<tr>
<td>CVE-2021-45105</td>
<td>Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial-of-service when a crafted string is interpreted.</td>
</tr>
</tbody>
</table>
Recommended Immediate Actions

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

<table>
<thead>
<tr>
<th>Affected Version</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSB v6</td>
<td>Patch is available. Please apply the patch or follow the General Mitigation Factors/Workarounds described below. Patch availability can be requested via the respective Customer Experience team.</td>
</tr>
</tbody>
</table>

General Mitigation Factors/Workarounds

Recommended security practices, Operating Systems hardening, and firewall configurations can help protect a user’s computer from the attacks. An entry point for this vulnerability is the unsecured Operating System on which the product is installed. We recommend hardening the Operating System accordingly. One recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” [https://www.cisecurity.org/about-us/](https://www.cisecurity.org/about-us/)

More information on the CIS recommended practices can be found in the following documents:

- CIS Benchmark v1.11.0-07-16-2021 for Microsoft Windows 10 Operating System [https://www.cisecurity.org/benchmark/microsoft_windows_desktop/](https://www.cisecurity.org/benchmark/microsoft_windows_desktop/)

Each recommendation within a CIS Benchmark is assigned a Level 1 or Level 2 profile. Each organization may choose which recommendation to implement based on the organization cybersecurity requirements.

Additional hardening guidelines or CIS Benchmarks are published for Microsoft Office, Microsoft 365, Google Chrome, Microsoft Web Browser at [https://www.cisecurity.org/cis-benchmarks/](https://www.cisecurity.org/cis-benchmarks/).

Routinely monitor the application process log for unrecognized user sessions originating from outside the application.

Frequently Asked Questions

What is Counterparty Settlement and Billing (CSB)?

Counterparty Settlements and Billing (CSB) is a software system used by market operators, utilities, and energy marketers to perform wholesale billing and settlement functions.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can insert and run arbitrary code on the CSB application 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 is being exploited in the wild. Hitachi Energy is not aware of this vulnerability having been exploited on a CSB installation.

**References**


**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**

<table>
<thead>
<tr>
<th>Date of the Revision</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-12-19</td>
<td>A</td>
<td>Initial public release.</td>
</tr>
<tr>
<td>2021-12-21</td>
<td>B</td>
<td>Add additional info CVE-2021-45046</td>
</tr>
<tr>
<td>2021-12-23</td>
<td>C</td>
<td>Add additional info CVE-2021-45105</td>
</tr>
</tbody>
</table>