REVISION: A
PUBLICATION DATE: 2022-05-02
DOC. IDENTIFIER: 8DBD000105
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Spring4Shell and Spring Framework Related Vulnerabilities in Hitachi Energy's Lumada APM's Prognostic Model Executor Service

CVE-2022-22950
CVE-2022-22965

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of public reports of Spring4Shell vulnerability (CVD-2022-22965) and a vulnerability affecting Spring Framework (CVE-2022-22950). The vulnerabilities affect the Prognostic Model Executor that is included in the Lumada APM product versions listed below. Note that the Prognostic Model Executor is not enabled by default. Please consult the Recommended Immediate Action Section for either remediation or mitigation strategy

An attacker who successfully exploited these vulnerabilities could cause the Prognostic Model Executor to fail and to run some arbitrary code.

Affected Products and Versions

List of affected products and product versions:

- Lumada APM on-line service (SaaS) version 6.3.220323.0 and prior.
- Lumada APM versions 6.0.0.0 to 6.0.0.4.
- Lumada APM versions 6.1.0.0 and 6.1.0.1.
- Lumada APM versions 6.2.0.0 to 6.2.0.2.
- Lumada APM versions 6.3.0.0 to 6.3.0.2.

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-2022-22950 CVSS v3.1 Base Score: 3.1 Low CVSS v3.1 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:X Link to NVD: click here	A vulnerability exists in the Spring Framework component included in the Prognostic Model Executor service of the Lumada APM product versions listed above. There may be a possibility for an attacker to leverage the application-provided SPeL expression to exploit this vulnerability by sending a specially crafted data or configuration to the application (directly or via integrated applications), causing the Prognostic Model Executor service to fail.
CVE-2022-22965 CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:X Link to NVD: click here	A vulnerability exists in the Spring Framework component included in the Prognostic Model Executor service of the Lumada APM product versions listed above. Given the nature of the vulnerability that is considered more general, there may be a possibility that an attacker could exploit the vulnerability by sending a specially crafted data or configuration to the application (directly or via integrated applications), causing the Prognostic Model Executor service to run arbitrary inserted code.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Lumada APM on-line service (SaaS)	None – all the SaaS environments of Lumada APM were already patched by Hitachi Energy.
Lumada APM versions 6.0.0.0 to 6.0.0.4	Apply patch version 6.0.0.5 (when available) or upgrade to a newer, unaffected, release version (e.g., 6.2.0.3) – subject to the license/service agreement.
Lumada APM versions 6.1.0.0 and 6.1.0.1	Apply patch version 6.1.0.2 (when available) or upgrade to a newer, unaffected, release version (e.g., 6.2.0.3) – subject to the license /service agreement.
Lumada APM versions 6.2.0.0 to 6.2.0.2	Apply patch version 6.2.0.4 or upgrade to a newer, unaffected, release version (e.g., 6.4.0.0) – subject to the license /service agreement.
Lumada APM versions 6.3.0.0 to 6.3.0.2	Apply patch version 6.3.0.3 (when available) or upgrade to a newer, unaffected, release version (e.g., 6.4.0.0) – subject to the license /service agreement.

Hitachi Energy recommends that customers apply the update at the earliest convenience. The update removes the vulnerability by updating the affected Spring component libraries to unaffected versions.

If a patch for a specific release version or a newer supported release version is not available, please apply the mitigation factors / workarounds listed below and monitor for patch releases for relevant release versions.

Mitigation Factors/Workarounds

Workaround

Hitachi Energy has tested the following workaround:

- **Disable the Prognostic Model Executor service**, by scaling it down to zero instances. Follow the installation guide instructions on how to perform this action.

Given that the vulnerabilities affect only the Prognostic Model Executor service, it is recommended to disable it if it is not used. By default, the Prognostic Model Executor is not enabled.

Impact of Workaround

- Disabling the Prognostic Model Executor service will cause the Lumada APM application to stop performing condition assessment calculations (for all assets configured to use prognostic models) and to accumulate calculation requests in the internal messaging queue. As the requests in the queue have a limited lifetime (set by messaging bus topic retention), when that lifetime expires, the request will be lost.
- When the Prognostic Model Executor service is restored to function (after applying the suggested remediation steps and according to the installation guide) it will start processing the accumulated requests. When the period of accumulation is long, this may result in a prolonged period of intensive calculations.

- If any requests were lost, the affected assets may be missing historical or even current condition assessments. To ensure the current assessments are up to date, the customer should trigger recalculation of condition of all assets using the performance models.

General Mitigation Factor

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.

Additional recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System.

As exploitation of this potential vulnerability requires “Administrator” role or “Import” role privileges for Lumada APM access or access to systems being the source of the data for the Lumada APM application, via integration API-s, the access to those role privileges and applications should be limited (following the least privilege principle) and controlled.

Hitachi Energy has tested the following workaround:

- **Disable the Prognostic Model Executor service**, by scaling it down to zero instances. Follow the installation guide instructions on how to perform this action.

Impact of Workaround

- Disabling the Prognostic Model Executor service will cause the Lumada APM application to stop performing condition assessment calculations (for all assets configured to use prognostic models) and to accumulate calculation requests in the internal messaging queue. As the requests in the queue have a limited lifetime (set by messaging bus topic retention), when that lifetime expires, the request will be lost.
  When the Prognostic Model Executor service is restored to function (after applying the suggested remediation steps and according to the installation guide) it will start processing the accumulated requests. When the period of accumulation is long, this may result in a prolonged period of intensive calculations.
  If any requests were lost, the affected assets may be missing historical or even current condition assessments. To ensure the current assessments are up to date, the customer should trigger recalculation of condition of all assets using the performance models.

Frequently Asked Questions

What is Lumada APM?

Lumada APM is an Asset Performance Management application, offered both as a service (in SaaS model) or as a customer-installable (on-premises) product. It’s a business analysis tool with web-based front-end and integration points. In SaaS model, it’s offered via public Internet.

What are Prognostic Models?

The core part of Lumada APM functionality is assessment of condition of the assets monitored within the application, implemented by various mathematical models. One of those is the prognostic model engine, providing the ability to build and execute prognostic models based on input data trends and anomalies, providing assessments and prognosis of defined malfunctions.

What is the Prognostic Model Executor service?

Prognostic Model Executor (PME) service is one of the Lumada APM internal services. It's responsible for fulfilling requests for prognostic model calculations, i.e., executing the prognostic models for the data accumulated by the application. It is a Java-based service using the Spring Framework.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could exploit these vulnerabilities to run arbitrary code on the system (which may lead to take control of the system, extracting sensitive data from it, etc.) or cause parts of the application functionalities (prognostic model asset condition assessments) to stop.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by using privileged access to the application's REST API-s (or to integrated applications, being sources of data for Lumada APM) to provide specially crafted data to the Lumada APM application, for the assets utilizing the prognostic models or specially crafted configuration data for those models. As a result, this may cause the Prognostic Model Executor to fail or run arbitrary code within the service.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected Lumada APM instance could exploit this vulnerability.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

Yes, the vulnerabilities in the Spring Framework, potentially affecting Lumada APM have been publicly disclosed. 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 Hitachi Energy received any report that this vulnerability was being exploited?

Hitachi Energy has observed different reports on exploitation attempts targeting Spring4Shell vulnerability. However, there was no report on it being exploited in our product.

References

1. https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and
2. https://tanzu.vmware.com/security/cve-2022-22965
3. https://tanzu.vmware.com/security/cve-2022-22950
4. https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement#am-i-impacted

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

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
2022-05-02	A	Initial public release.