TLP: CLEAR
REVISION: 1
PUBLICATION DATE: 2022-12-13
DOC. IDENTIFIER: 8DBD000112
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Incomplete Access Control Vulnerability in User Asset Group Feature of Hitachi Energy's Lumada APM Product

CVE-2022-2155

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of an internal report of a vulnerability in the Lumada APM's User Asset Group implementation, allowing a limited-access user to access data or features, which should be unavailable to the limited-access user. Please consult the Recommended Immediate Actions for remediation and mitigation steps.

An attacker who successfully exploited this vulnerability could read data, which should be unavailable by gaining access to any Power BI report installed or manipulate asset issue comments in Lumada APM of the assets, the user is not authorized to access.

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-2022-2155 CVSS v3.1 Base Score: 5.7 - Medium CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N Link to NVD: click here	• A vulnerability exists in the Lumada APM's User Asset Group feature due to a flaw in access control mechanism implementation on the "Limited Engineer" role, granting it access to the embedded Power BI reports feature. An attacker that manages to exploit the vulnerability on a customer's Lumada APM could access unauthorized information by gaining unauthorized access to any Power BI reports installed by the customer. • Another flaw enables a user authorized to manipulate asset issue comment, to manipulate all asset issue comments, regardless of the User Asset Group limitations. An attacker that manages to exploit the vulnerability on a customer's Lumada APM could manipulate asset issue comments on assets, which should not be available to that user.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Lumada APM – SaaS version version 6.0.0.0 to 6.4.220601.0	The SaaS environment is remediated as of Lumada APM – SaaS version 6.5.0.0. No action required from customers.
Lumada APM – On Premises versions 6.0.0.0 to 6.4.0.*	• For Lumada APM version 6.4.0.* – Update to Lumada APM version 6.4.0.1, or upgrade to Lumada APM version 6.5.0.0 (or newer).. • For Lumada APM versions prior to 6.4.0.0 – Upgrade to Lumada APM version 6.4.0.1 or 6.5.0.0 or newer. Remediation for versions 6.3, 6.2 and 6.1 are planned for release later If upgrade is not possible and a patch not available for your version, please apply mitigation factors. See Section Mitigation Factors/Workarounds. Note that Lumada APM version 6.5.0.0 and newer are not vulnerable.

Mitigation Factors/Workarounds

Out-of-the-box, Lumada APM – On Premise does not support the Power BI integration feature. Nonetheless, one can connect a subscription-based Power BI to Lumada APM.

- In case the Power BI integration feature is enabled, it is recommended to either disable the unsupported Power BI integration feature if there are users with “Limited Engineer” role, or to remove the any users with “Limited Engineer” role or to assign those users to other role prior to using the unsupported Power BI integration feature.
- If Power BI integration is disabled, it is safe to continue to assign the “Limited Engineer” role to users.

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 Lumada Asset Performance Management (APM)?

Lumada APM is a solution for enterprise level customers (not mass market) allowing centralized, high-level analytics of assets fleet condition. It is a web-based solution offered both as a cloud-based service (Soft-ware-as-a-Service), as well as an “on premises” variant. It is deployed on Epiphany platform – a unified set of software components for microservice oriented applications.

What are the User Asset Groups?

User Asset Groups is a security feature of Lumada APM designed to allow the customer to segregate the assets monitored in a Lumada APM to groups and map them to Security Groups of application users, to limit users’ access to only assets belonging to a single group. Users belonging to such groups, so with limited access to assets, are referred to here as limited access users.

Is the User Asset Groups feature enabled for all Lumada APM instances?

User Asset Groups security feature is an opt-in feature, i.e. by default set to be dormant/disabled. This means, that, by default, no limitations are applied and all the application users, regardless to what Security Groups they belong, have access to all assets monitored in the Lumada APM application instance.

What is the Limited Engineer user role for?

Support for User Asset Group security feature limitations was introduced in Lumada APM gradually. Which means, that not all business features of Lumada APM are applying the limitations. Depending on the Lumada APM version, the subset of the features supporting the limitation differs. Additionally, not all features can support the limitations. For those reasons, a Limited Engineer role was made available, to support the User Asset Groups feature. This role offers a subset of features available to the Engineer role, where the available features are those, which support the User Asset Group feature limitations.

For the User Asset Groups feature to be fully effective, the customer should be applying the Limited Engineer role to all limited access users (i.e. without intended access to all the monitored assets).

Depending on the application version, there may be other “Limited” user roles available (e.g. Limited Administrator) supporting the feature with a different subset of features available to a user.

What is the Power BI integration feature?

Lumada APM SaaS variant offers support for embedded Power BI reports. This allows the customer to design custom reports, containing dashboards, summaries, etc., upload them to Lumada APM and have them available to their users, without having to use otherwise paid features of Power BI services.

The embedded Power BI reporting feature is only intended for use in the SaaS version of APM, however it may be possible to configure an on-premises installation of Lumada APM to use that feature. Such configuration and use is however not supported by Hitachi Energy.

What might an attacker use the vulnerability to do?

An attacker that manages to exploit the vulnerability in access to Power BI reports, on a customer’s Lumada APM could access unauthorized information by gaining unauthorized access to any Power BI reports installed for that particular customer. As the Limited Engineer role does not allow a user to install Power BI reports in Lumada APM, the user would not be able to extend their scope of view on the asset fleet beyond what is covered by existing reports or reports added by other users.

An attacker that manages to exploit the vulnerability in access to asset issue comments could post (create) comments to issues of those assets, which are not intended to be available to the attacker.

How could an attacker exploit the vulnerability?

On a Lumada APM on-premises instance, with the (unsupported) Power BI reporting integration enabled, an authenticated attacker could try to exploit the vulnerability by manipulating the Lumada APM UI to access any Power BI report deployed on that instance and manipulating (clearing) the report filters.

On any Lumada APM on-premises instance, an attacker could try to directly call application API-s, designed to support the application UI, and use enumeration techniques, to guess asset issue identifiers and thus generate API calls to create comments on any asset issues.

Could the vulnerability be exploited remotely?

The vulnerability is not bound to a network stack. To exploit this vulnerability an attacker would need to gain access to the APM’s web interface of the affected system of which the Power BI feature is enabled.

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

No, the vulnerability is reported internally and had not been publicly disclosed.

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

No, Hitachi Energy had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

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
2022-12-13	1	Initial public release.

DocuSigned by: