TLP: CLEAR
REVISION: 1
PUBLICATION DATE: 2022-12-13
DOC. IDENTIFIER: 8DBD000134
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

OpenSSL and Zlib Related Vulnerabilities in Hitachi Energy's Lumada Asset Performance Management (APM) Product

CVE-2022-3602
CVE-2022-3786
CVE-2022-37434

Notice

Hitachi Energy

Summary

Hitachi Energy is aware multiple vulnerabilities related to components OpenSSL library (versions from 3.0.0 to 3.0.6) and zlib that are used in the product versions listed below. Successful exploitation may cause a denial-of-service. For affected versions and immediate mitigation/workaround information, please refer to the Mitigation Factors/Workaround Section below.

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-2022-3602 CVSS v3.1 Base Score: 7.5 - High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. In Lumada APM, this can be triggered by configuring APM to connect to a malicious server for one of the supported integrations. This may cause a crash of the specific APM service implementing the integration (causing a denial of service).
CVE-2022-3786 CVSS v3.1 Base Score: 7.5 - High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. In Lumada APM, this can be triggered by configuring APM to connect to a malicious server for one of the supported integrations. This may cause a crash of the specific APM service implementing the integration (causing a denial of service).
CVE-2022-37434 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	A security vulnerability was found in the affected version of zlib. Successful exploitation of this vulnerability may result in denial of service or potentially the execution of arbitrary code.

Recommended Immediate Actions

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

Vulnerabilities	Affected Version	Recommended Actions
OpenSSL vulnerabilities **CVE-2022-3602** **CVE-2022-3786**	Lumada APM SaaS	No action is required by customers. Hitachi Energy has remediated the vulnerability in the Hitachi Energy managed SaaS environments.
	Lumada APM On-premises version 6.5.0.0	The vulnerabilities are remediated in: • Lumada APM version 6.5.0.1 Please update to the remediated versions or apply mitigation as described in Section Mitigation Factors/Workarounds.
Zlib vulnerability **CVE-2022-37434**	Lumada APM SaaS	No action is required by customers. Hitachi Energy has remediated the vulnerability in the Hitachi Energy managed SaaS environments.
	Lumada APM On-premises version 6.5.0.0 and versions between 6.1.0.0* and 6.4.0.0	The vulnerability is remediated in: • Lumada APM version 6.5.0.1 • Lumada APM version 6.4.0.1. Please update or upgrade to the remediated versions accordingly or apply mitigation as described in Section Mitigation Factors/Workarounds.

** The versions prior to 6.1.0.0 are no longer supported and were not assessed for the vulnerabilities.*

Mitigation Factors/Workarounds

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, have security updates applied to installed software components and others that must 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 (Software-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 might an attacker use the OpenSSL vulnerability to do?

An attacker who successfully exploited this vulnerability in Lumada APM services could potentially be able to cause some Lumada APM services to stop or become inaccessible, causing some or all Lumada APM functionality to become unavailable.

How could an attacker exploit the OpenSSL v3.x vulnerabilities?

To exploit the vulnerabilities in Lumada APM application installation, the attacker would need to force APM to communicate with a service, which uses a maliciously crafted TLS certificate, by configuring one of Lumada APM integrations to refer to that service's address. This would require authenticated access to APM's user interface (with Administrator role) or to APM's integration API-s (with Import or Super Admin role).

Limiting access to APM would help to mitigate such attacks. Also see sections for recommended actions for Epiphany platform, Mitigating Factors and General Mitigation Factors above.

What might an attacker use the zlib vulnerability to do?

An attacker who successfully exploited this vulnerability in Lumada APM services could potentially be able to cause some Lumada APM services to stop or become inaccessible, causing some or all Lumada APM functionality to become unavailable or cause an arbitrary code being executed by the Lumada APM services.

How could an attacker exploit the zlib vulnerability?

To exploit the vulnerability in Lumada APM application installation (via vulnerability in the Lumada APM services or the Epiphany platform components), the attacker would need to send a malicious compressed payload to Lumada APM HTTP endpoints (including REST API endpoints).

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to affected system nodes 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 OpenSSL v3.x and zlib vulnerabilities have been publicly disclosed by their respective authors.

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

Based on available information, Hitachi Energy is not aware that these vulnerabilities are being exploited.

References

- NVD - CVE-2022-3602 (nist.gov)
- NVD - CVE-2022-3786 (nist.gov)
- NVD - CVE-2022-37434 (nist.gov)
- OpenSSL Security Advisory [01 November 2022]
- USN-5710-1: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu

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
2022-12-13	1	Initial public release.

DocuSigned by: