TLP: WHITE
REVISION: 1
PUBLICATION DATE: 2022-12-06
DOC. IDENTIFIER: 8DBD000137
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

OpenSSL v3.x Related Vulnerabilities in Hitachi Energy's Network Manager Process Communication Unit PCU400 Product

CVE-2022-3602
CVE-2022-3786

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of two vulnerabilities CVE-2022-3602 and CVE-2022-3786 in OpenSSL library (versions from 3.0.0 to 3.0.6) which are used in the PCU400 product versions listed below. Successful exploitation may cause a denial-of-service of the PCU400 Logger and PCUCAG server. The product versions listed in this document are affected by the 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.

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 PCU400, this vulnerability could be exploited if a malicious TLS certificate is used to secure communication between PCU400 and PCULogger. Successful exploitation may cause a denial-of-service of the PCU400 Logger and PCUCAG server. Note, the issue is related to logging with the PCULogger tool otherwise the PCU system is not impacted.
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 PCU400, this vulnerability could be exploited if a malicious TLS certificate is used to secure communication between PCU400 and PCULogger. Successful exploitation may cause a denial-of-service of the PCU400 Logger and PCUCAG server. Note, the issue is related to logging with the PCULogger tool otherwise the PCU system is not impacted.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
PCU400 v9.3.x	Remediated in PCU v9.4 and PCU v9.3.8. Please update to the remediated versions or apply general mitigation factors. For more details, please contact your Client Advocate.
PCULogger v1.0.1	Remediated in PCULogger v1.1.0. Please update to the remediated versions or apply general mitigation factors. For more details, please contact your Client Advocate.

General 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 Network Manager Process Communication Unit PCU400?

PCU400 is the Data Acquisition system for Network Manager.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could potentially cause a crash of the PCUCAG server.

How could an attacker exploit the vulnerability?

To exploit the vulnerability in PCU400 Logger, an attacker needs to craft an SSL/TLS certificate with a malicious E-Mail address fulfilling the condition of exploitation. It is important to ensure the SSL/TLS certificate is properly generated by the authorized organization within customer’s authority. Furthermore, limiting access to PCU400 in general would help to mitigate such attacks. Also see sections for recommended actions for Mitigating Factors and General Mitigation Factors above.

Could the vulnerability be exploited remotely?

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 vulnerabilities have been publicly disclosed by OpenSSL team.

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)
- OpenSSL Security Advisory [01 November 2022]

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
2022-12-06	1	Initial public release.

DocuSigned by: