TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-02-14
DOC. IDENTIFIER: 8DBD000118
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

CYBERSECURITY ADVISORY

Multiple Open-Source Software Vulnerabilities in Hitachi Energy's Gateway Station (GWS) Product

CVE-2022-0778
CVE-2020-25692

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 publicly available vulnerability reports on various open-source software, i.e, OpenLDAP and OpenSSL that are used in the Gateway Station (GWS) products versions listed in the Recommended Actions Section. An update is available that remediates the vulnerabilities in the products.

An attacker who successfully exploited the vulnerabilities could cause the affected modules in the product to stop working.

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-2020-25692 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 NULL pointer dereference was found in affected version of OpenLDAP. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial-of-Service on the user authentication function. Nonetheless, the local authentication will continue to work. Note that the authentication service is not installed by default.
CVE-2022-0778 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 vulnerability exists in the OpenSSL's BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. Successful exploitation may cause a denial-of-service.

Recommended Immediate Actions

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

Vulnerabilities	Affected Version	Recommended Actions
CVE-2020-25692	GWS 2.0.0.0, GWS 2.1.0.0, GWS 2.2.0.0, GWS 2.3.0.0, GWS 2.4.0.0, GWS 3.0.0.0 and GWS 3.1.0.0 (if Authentication Service is installed – See Mitigation Information)	Remediated as of GWS 3.2.0.0 version Recommended to update to GWS 3.3.0.0 version Or apply general mitigation factors
CVE-2022-0778	GWS 3.2.0.0 and earlier	Remediated in GWS 3.3.0.0 version Update to at least GWS 3.3.0.0 version Or apply general mitigation factors.

Hitachi Energy recommends that customers apply the update at the earliest convenience.

Mitigation Factors/Workarounds

For CVE-2020-25692, the vulnerability impacts GWS if the Authentication Service is installed. It is not installed by default but needs to be either enabled during the installation process of GWS or installed manually later. Authentication Service (previously ABB Authentication Service) is needed only when GWS users are authenticated using centralized SDM600 user account management.

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 Gateway Station (GWS) Product?

Gateway Station (GWS) is a product, which is used for monitoring and controlling HVDC stations.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected functions in the system node become inaccessible.

How could an attacker exploit the vulnerability?

An attacker first needs to gain access to the network in which an affected system node resides, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Next, an attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to the affected system node. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

An attacker who has a 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, these vulnerabilities have been publicly disclosed by the respective Open-Source Software teams.

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 these vulnerabilities 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
2023-02-14	1	Initial public release.

DocuSigned by:

Issued by: Hitachi Energy

Hitachi Energy

Product Security Incident Response Team