

CYBERSECURITY ADVISORY

# Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy Gateway Station (GWS) Product

CVE-2020-1968

CVE-2020-8252

CVE-2020-8172

CVE-2020-8265

CVE-2020-8174

CVE-2020-8287

CVE-2020-8201

## 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 internal reports of multiple open-source software related vulnerabilities in the Gateway Station (GWS) product versions listed in this document. Remediated versions are available that remediate the identified vulnerabilities.

An attacker who successfully exploited this vulnerability could eavesdrop on the traffic between network source and destination, gain unauthorized access to information or cause a denial-of service.

## 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.

### OpenSSL

CVE-ID	Severity, Vector and Link to NVD
CVE-2020-1968	CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click <a href="#">here</a>

### Node.JS

CVE-ID	Severity, Vector and Link to NVD
CVE-2020-8172	CVSS v3.1 Base Score: 7.4 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N Link to NVD: click <a href="#">here</a>
CVE-2020-8174	CVSS v3.1 Base Score: 8.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click <a href="#">here</a>
CVE-2020-8201	CVSS v3.1 Base Score: 7.4 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N Link to NVD: click <a href="#">here</a>
CVE-2020-8252	CVSS v3.1 Base Score: 7.8 High CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Link to NVD: click <a href="#">here</a>
CVE-2020-8265	CVSS v3.1 Base Score: 8.1 High CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click <a href="#">here</a>
CVE-2020-8287	CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Link to NVD: click <a href="#">here</a>

Below follows a summary regarding the possible impact of the identified vulnerabilities:

- **OpenSSL vulnerability:** Exploitation of the OpenSSL Raccoon attack may allow an attacker to compute the pre-master secret between the client and server in connections which have used a Diffie-Hellman (DH) based cipher suite and thus able to eavesdrop on all encrypted communications sent over that TLS connection.
- **Node.js vulnerabilities:** Exploitation may cause a denial-of-service to the system, data extraction by various methods, bypass the hostname checks in TLS connections or memory corruption.

## Affected Product Versions & Recommended Immediate Actions

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

Affected Version	Recommended Actions
GWS 2.0.0.0 and earlier	Apply the mitigation factors as described in the Section General Mitigation Factors/Workaround.
GWS 2.1.0.0	
GWS 2.2.0.0	A remediated version GWS 3.2.0.0 is currently being planned.
GWS 2.3.0.0	
GWS 2.4.0.0	
GWS 3.0.0.0	For update or upgrades, please get in touch with your local Hitachi Energy contacts.
GWS 3.1.0.0	

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

## 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, 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 eavesdrops on the traffic, cause the affected system node to stop or become inaccessible / allow the attacker to access to information without proper access rights.

## How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. Some vulnerabilities described above also require authentication to the system before they can be exploited.

Exploitation would require the attacker to have access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or through an installed malicious software on a system node. Recommended practices help to mitigate such attacks, see section Mitigating Factors above.

## Could the vulnerability be exploited remotely?

Yes, 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, at the time of this advisory publication Hitachi Energy had not received any information indicating that this vulnerability had been exploited.

## 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](mailto:cybersecurity@hitachienergy.com)

## Revision

Date of the Revision	Revision	Description
2022-05-03	A	Initial public release.