

## CYBERSECURITY ADVISORY

# Multiple Vulnerabilities in Hitachi Energy's Gateway Station (GWS) Product

CVE-2022-1778

CVE-2022-2277

CVE-2022-29922

CVE-2022-29492

## 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 vulnerabilities in the Gateway Station (GWS) versions as described in the Recommended Immediate Actions Section below. An update is available that resolves the reported vulnerabilities.

An attacker who successfully exploited the vulnerabilities, depends on the vulnerabilities, could cause part of GWS fail to start, unauthorized actor to run scripts, and may 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.

Vulnerability ID	Detail Description
<p><b>CVE-2022-1778</b>            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 <a href="#">here</a></p>	<p>A vulnerability exists during the start of GWS, where an input validation flaw causes a buffer-overflow while reading a specific configuration file. Subsequently GWS will fail to start. The configuration file can only be accessed by an administrator access.</p>
<p><b>CVE-2022-2277</b>            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 <a href="#">here</a></p>	<p>A vulnerability exists in the ICCP stack due to validation flaw in the process that establishes the ICCP communication. The validation flaw will cause a denial-of-service when ICCP of SYS600 is requested to forward any data item updates with timestamps too distant in the future to any remote ICCP system. By default, ICCP is not configured and not enabled.</p>
<p><b>CVE-2022-29492</b>            CVSS v3.1 Base Score: 5.3 Medium            CVSS v3.1 Vector:            AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/            Link to NVD: click <a href="#">here</a></p>	<p>A vulnerability exists in the handling of a malformed IEC 104 TCP packet. Upon receiving a malformed IEC 104 TCP packet, the malformed packet is dropped, however the TCP connection is left open. This may cause a denial-of-service if the affected connection is left open.</p>
<p><b>CVE-2022-29922</b>            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 <a href="#">here</a></p>	<p>A vulnerability exists in the handling of a specially crafted IEC 61850 packet with a valid data item but with incorrect data type in the IEC 61850 OPC Server. The vulnerability may cause a denial-of-service on the IEC 61850 OPC Server part of the GWS product.</p>

## Recommended Immediate Actions

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

Vulnerabilities	Affected Version	Recommended Actions
CVE-2022-1778	GWS 3.0.0.0	Remediated in GWS 3.3.0.0 version
	GWS 3.1.0.0	Update to at least GWS 3.3.0.0 version
	GWS 3.2.0.0	Or apply general mitigation factors
CVE-2022-2277	GWS 3.1.0.0	Remediated in GWS 3.3.0.0 version
	GWS 3.2.0.0	Update to at least GWS 3.3.0.0 version
		Or apply general mitigation factors Do not enable ICCP if it is not used
CVE-2022-29492 CVE-2022-29922	GWS 3.1.0.0 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.

## 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. Proper password policies and processes should be followed.

## 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 the CVE-2022-1778 could cause a failure in starting part of GWS. When CVE-2022-29490 vulnerability is exploited, an attacker could run an administrator level script that could provide the attacker access to information and to cause a disruption in GWS operation. For the CVE-2022-2277, CVE-2022-29492 and CVE-2022-29922, upon successful exploitation, an attacker could cause a denial-of-service on the respective function in GWS.

### How could an attacker exploit the vulnerability?

To exploit CVE-2022-1778, an attacker needs to have a local access to the GWS and an administrator account is required.

For CVE-2022-2277, if ICCP is configured and enabled in GWS, an attacker needs to send data item updates with timestamps too distant in the future to a GWS server which is configured to forward the data via ICCP to other ICCP clients.

CVE-2022-29492 and CVE-2022-29922, can be exploited without authentication by sending malicious packets over the network towards the affected GWS instance.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

## Could the vulnerability be exploited remotely?

For CVE-2022-1778, an attacker needs to gain an access to the server where GWS is installed. For the CVE-2022-2277, CVE-2022-29492 and CVE-2022-29922, these vulnerabilities are bound to a network stack. This means, exploitation would require that the attacker has access to the system network, 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. 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.

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

## Revision

Date of the Revision	Revision	Description
2023-02-14	1	Initial public release.

DocuSigned by:

