Cybersecurity Advisory – Specially Crafted IEC 61850 Protocol Sequence Vulnerability in GMS600

CVE-2021-27196

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi ABB Power Grids. Hitachi ABB Power Grids 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 ABB Power Grids 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 ABB Power Grids 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 ABB Power Grids 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.

Affected Products and versions

GMS600 Versions 1.3.0 and before

Vulnerability ID

CVE ID: CVE-2021-27196

Summary

A privately reported vulnerability in which an attacker having access to the IEC 61850 network with knowledge on how to reproduce the attack and knowing the IP addresses of the different IEC 61850 access points (of IEDs/products) can reproduce this attack and force the GMS600 to reboot putting it out of operation for around 60 seconds. Consequently, there will be a gap in recorded operations happening during the reboot and missing or false status indication on connected clients reading and/or displaying data retrieved from the GMS600.

An attacker who successfully exploited this vulnerability could reboot the device regularly or according to a scheme that would lead to repeated cases as described above resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	7.2
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C&version=3.1

Vulnerability Details

A vulnerability exists in the command handling of the device included in the product revisions listed above. An attacker could exploit the vulnerability by using specially crafted message and force the device to reboot. During reboot, the primary functionality is not available with the consequences described as above.

Recommended immediate actions

The problem is corrected in the following product versions:

GMS600 version 1.3.1

Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience.

Mitigation Factors

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.

More information on recommended practices can be found in the Cybersecurity Deployment Guidelines for each product version.

Workarounds

Not connecting the GMS600 to any station network through the LAN port (optical or RJ45) should make above attack physically impossible. The primary functionality of the GMS600 will remain fully intact in this case, but no remote reading of the data over Ethernet-based protocols would be possible.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could reboot the device resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available resulting in the consequences described above.

What causes the vulnerability?

The vulnerability is caused by a weakness in the message processing in the IEC 61850 protocol.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could reboot the device resulting in a denial of service situation. During the reboot phase, the primary functionality of the device is not available with the consequences described above.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This 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 fire-wall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has 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.

What does the update do?

The update mitigates the identified weakness in the IEC 61850 protocol.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, Hitachi ABB Power Grids received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had Hitachi ABB Power Grids received any reports that this vulnerability was being exploited?

No, Hitachi ABB Power Grids had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

Hitachi ABB Power Grids thanks the following for working with us to help protect customers:

- Markus Mahrla, GAI NetConsult GmbH
- Lars Lengersdorf, Amprion GmbH

Support

For additional information and support please contact your product provider or Hitachi ABB Power Grids service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi ABB Power Grids contact-centers.