REVISION: A
PUBLICATION DATE: 2021-11-04
DOC. IDENTIFIER: 8DBD000059
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Insufficient Security Control Vulnerability in Hitachi Energy GMS600 Product

CVE-2021-35534

Notice

Summary

Hitachi Energy is aware of a vulnerability report from U.S. Department of Energy CyTRICS researcher of a vulnerability in the GMS600 product version listed below. Recommended action for each affected version is listed in the Recommended Immediate Actions Section.

An attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product.

Affected Products and Versions

List of affected products and product versions:

- GMS600 v1.2.0
- GMS600 v1.3.0
- GMS600 v1.3.1.0

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-2021-35534 CVSS v3.1 Base Score: 7.2 High CVSS v3.1 Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	A vulnerability exists in the database schema inside the product versions listed above. An attacker could exploit the vulnerability by first gaining access to credentials of any account or to have access to a session ticket issued for an account. After that, via the configuration tool that accesses the proprietary Open Database Connectivity (ODBC) protocol (TCP 2102), the database table can be manipulated for privilege escalation which then allowed unauthorized modification or to permanently disabling of the device.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
GMS600 v1.2.0	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy.
GMS600 v1.3.0	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy.
GMS600 v1.3.1.0	Please refer to the Mitigation Factors/Workaround Section for the current mitigation strategy.

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 must be evaluated case by case. For instance, Open Database Connectivity (ODBC) protocol that is used for device configuration should be limited within the substation only.

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 GMS600?

Hitachi Energy GMS600 is a monitoring device for Generator Circuit-Breakers (GCBs). It collects several sensor measurements, current and voltages, records operations, logs data and events and uses its built-in functionality to make the collected information accessible to users via internet-based communication protocols and a local HMI. It also performs several calculations on selected data to enable predictive statements on various performance indicators of the GCB. The GMS600 is configured for each GCB individually, this configuration data is saved in a built-in database.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could remotely grant privileges, do unauthorized modifications on data and firmware, gain code execution and permanently disable the product.

How could an attacker exploit the vulnerability?

To exploit the vulnerability, an attacker needs to gain access to any account/ticket and its credentials that has been assigned one of a known access role and to also have access to the device configuration tool that accesses the Open Database Connectivity protocol (ODBC) port (TCP 2102).

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 via the open ODBC port that is available at any connection points in the product. Recommended practices include restricting the usage of ODBC port only on front port (service interface) and 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?

No, Hitachi Energy received information about this vulnerability through responsible disclosure.

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 this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgement

Hitachi Energy thanks the following for working with us to help protect customers:

– U.S. Department of Energy CyTRICS researcher Robert Erbes.

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
2021-11-04	A	Initial public release.