

CYBERSECURITY ADVISORY

# **BadAlloc – Memory Allocation Vulnerabilities in Hitachi Energy GMS600 Product**

**CVE-2020-28895**

**CVE-2020-35198**

## **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 two critical memory allocation vulnerabilities (called BadAlloc [1] vulnerabilities) in the WindRiver VxWorks Operating Systems [2][3] that are used in our product versions listed above.

An attacker that exploits these vulnerabilities might bypass security controls to execute malicious code or cause a denial-of-service. For immediate mitigation/workaround information, please refer to the Mitigation Factors/Workaround Section below.

## Affected Products and Versions

List of affected products and product versions:

GMS600 v1.2.0

GMS600 v1.3.0

GMS500 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
<b>CVE-2020-28895</b> CVSS v3.1 Base Score: 7.3 High CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L Link to NVD: click <a href="#">here</a>	In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by <code>calloc()</code> . As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
<b>CVE-2020-35198</b> CVSS v3.1 Base Score: 9.8 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click <a href="#">here</a>	An issue was discovered in Wind River VxWorks 7. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by <code>calloc()</code> . As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.

## Recommended Immediate Actions

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

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

## Mitigation Factors/Workarounds

Recommended security best practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include ensuring critical applications and 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. Firewalls should be configured to have the minimum number of ports exposed and open ports should be justified and documented. Critical 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. It is important to implement robust security awareness training to ensure users can identify common attacks or content such as phishing E-Mails or malicious web pages. Additionally, please refer to the mitigation strategy that is proposed by Microsoft Section 52 team [1] who discovered these vulnerabilities.

## Frequently Asked Questions

### What is Hitachi Energy 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 cause a denial-of-service and may be able to also execute malicious code on the device leading to incorrect operation by the device.

### Could the vulnerability be exploited remotely?

To the best of our knowledge and up to the time when this advisory is prepared, no known remote exploitation has been identified. However, we recommend following the recommended immediate action as described in this document to mitigate any potential exploit.

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

Yes, Hitachi Energy received information through a public disclosure that is released by Microsoft's Section 52 Team [1].

### 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.

## References

1. BadAlloc – Microsoft’s Section 52 - <https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/>
2. Wind River VxWorks – CVE-2020-28895 Advisory - <https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-28895>
3. Wind River VxWorks – CVE-2020-35198 Advisory - <https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-35198>

## 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<sup>1</sup> – [cybersecurity@hitachienergy.com](mailto:cybersecurity@hitachienergy.com) .

## Revision

Date of the Revision	Revision	Description
2021-12-16	A	Initial public release.

---

<sup>1</sup> Signature file of this PDF is available at <https://www.hitachienergy.com/cybersecurity/alerts-and-notifications>