REVISION: C
PUBLICATION DATE: 2022-01-27
DOC. IDENTIFIER: 9AKK107992A5975
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

BadAlloc – Memory Allocation Vulnerabilities in Hitachi Energy's Modular Switchgear Monitoring System (MSM) Product

CVE-2020-28895
CVE-2020-35198

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a 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 below.

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:

– Modular Switchgear Monitoring System MSM – version 2.1 or prior (running VxWorks v6.9)

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-2020-28895 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 here	In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
CVE-2020-35198 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 here	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 calloc(). 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
MSM – version 2.1 or prior (running VxWorks v6.9)	Upgrade to MSM version 2.2

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 are able to 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 MSM Product?

The Hitachi Energy Modular Switchgear Monitoring System is a product to monitor i.e., analyze condition of high-voltage switchgear like dead tank breakers (DTB), live tank breakers (LTB), gas-insulated switchgear (GIS) and Plug and Switch System (PASS) hybrid switchgear. Please refer Modular Switchgear Monitoring (MSM) (hitachiabb-powergrids.com) for more information about this product.

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.

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 firewall, 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?

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 – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2021-08-19	A	Initial public release.
2021-09-07	B	Update: • the Summary section – 2nd paragraph; • answer to FAQ 1st question
2022-01-27	C	Changed to Hitachi Energy's template Updated Recommended Immediate Actions: • A patch that remediates the vulnerability is available. Updated FAQs Section to harmonize with other relevant advisories. Corrected the affected version info.