

CYBERSECURITY ADVISORY

# **WindRiver VxWorks IPNet Vulnerabilities, Impact on Relion® 670, Relion 650, SAM600-IO Series**

CVE-2019-12256  
CVE-2019-12258  
CVE-2019-12259  
CVE-2019-12260  
CVE-2019-12261  
CVE-2019-12262  
CVE-2019-12263  
CVE-2019-12265

## **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

List of affected products and product versions:

Products and Affected Versions
1. Relion 670 series version 2.2.0.9 through version 2.2.0.12
2. Relion 670 series version 2.2.1.0 through version 2.2.1.5
3. Relion 670 series version 2.2.2.0 and version 2.2.2.2
4. Relion 670 series version 2.2.3.0 and version 2.2.3.1
5. Relion 650 series version 1.3.0.0 through version 1.3.0.6
6. Relion 650 series version 2.2.0.9 through version 2.2.0.12
7. Relion 650 series version 2.2.1.0 through version 2.2.1.5
8. Relion SAM600-IO version 2.2.1.0 through version 2.2.1.4

## Vulnerability ID

### CVE ID:

CVE-2019-12256, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12265

## Summary

On the July 29<sup>th</sup>, 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public. Hitachi ABB Power Grids Relion 670/650/SAM-IO series is affected by these vulnerabilities as listed above.

An attacker who successfully exploits these vulnerabilities could allow attackers to hijack existing TCP sessions to inject packets of their choosing or cause Denial-of-Service (DoS) attacks.

## Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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.

**CVE-2019-12256**                      Stack overflow in the parsing of IPv4 packets' IP options

CVSS v3 Base Score:                      9.8

CVSS v3 Temporal Score:                      8.8

CVSS v3 Vector:                              AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

CVSS v3 Link:                                [NVD Link](#)

**CVE-2019-12258** DoS of TCP connection via malformed TCP options

CVSS v3 Base Score: 7.5  
CVSS v3 Temporal Score: 6.7  
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12259** DoS via NULL dereference in IGMP parsing

CVSS v3 Base Score: 7.5  
CVSS v3 Temporal Score: 6.7  
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12260** TCP Urgent Pointer state confusion caused by malformed TCP AO option

CVSS v3 Base Score: 9.8  
CVSS v3 Temporal Score: 8.8  
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12261** TCP Urgent Pointer state confusion during connect() to a remote host

CVSS v3 Base Score: 8.8  
CVSS v3 Temporal Score: 7.9  
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12262** Handling of unsolicited Reverse ARP replies (Logical Flaw)

CVSS v3 Base Score: 7.1  
CVSS v3 Temporal Score: 6.4  
CVSS v3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12263** TCP Urgent Pointer state confusion due to race condition

CVSS v3 Base Score: 8.1  
CVSS v3 Temporal Score: 7.3  
CVSS v3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C  
CVSS v3 Link: [NVD Link](#)

**CVE-2019-12265** IGMP Information leak via IGMPv3 specific membership report

CVSS v3 Base Score: 5.3

CVSS v3 Temporal Score: 4.8

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

CVSS v3 Link: [NVD Link](#)

## Vulnerability Details

Relion 670/650/SAM600-IO product uses the TCP/IP stack from the operating system Wind River VxWorks. Several vulnerabilities exist in the VxWorks operating system included in the product versions listed above. An attacker who successfully exploits these vulnerabilities could allow attackers to hijack existing TCP sessions to inject packets of their choosing or cause Denial of Service (DoS) attacks.

<b>CVE ID</b>	<b>Detail Description</b>
<b>CVE-2019-12256:</b> Stack overflow in the parsing of IPv4 packets' IP options	By sending IPv4 packet with specially crafted options, an attacker could cause a crash the network task or execute arbitrary code.
<b>CVE-2019-12258:</b> DoS of TCP connection via malformed TCP options	By sending TCP packets with crafted TCP options, an attacker could cause the TCP-session to be reset, triggering a Denial-of-Service condition.
<b>CVE-2019-12260:</b> TCP Urgent Pointer state confusion caused by malformed TCP AO option	By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger a crash of the application or execute arbitrary code.
<b>CVE-2019-12261:</b> TCP Urgent Pointer state confusion during connect() to a remote host	By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger a crash of the application or execute arbitrary code.
<b>CVE-2019-12263:</b> TCP Urgent Pointer state confusion due to race condition	By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger race condition which could lead to execute arbitrary code.
<b>CVE-2019-12259:</b> DoS via NULL dereference in IGMP parsing	By sending specially crafted IGMP packets, an attacker could potentially trigger a Denial-of-Service condition.
<b>CVE-2019-12262:</b> Handling of unsolicited Reverse ARP replies (Logical Flaw)	An attacker with access to the network, could send reverse-ARP responses to the device. This vulnerability will not cause any harm more than increased usage of RAM. However, it could affect the availability of the device.
<b>CVE-2019-12265:</b> IGMP Information leak via IGMPv3 specific membership report	By sending specially crafted IGMPv3 packets, an attacker may be able to retrieve data from the targeted device.

## Recommended Immediate Versions

The issue is corrected in the following product versions:

Products and Fixed Versions	
1.	Relion 670 series version 2.2.0 → Fixed in version 670 2.2.0.13
2.	Relion 670 series version 2.2.1 → Fixed in version 670 2.2.1.6
3.	Relion 670 series version 2.2.2 → Fixed in version 670 2.2.2.3
4.	Relion 670 series version 2.2.3 → Fixed in version 670 2.2.3.2
5.	Relion 650 series version 1.3.0 → Fixed in version 650 1.3.0.7*
6.	Relion 650 series version 2.2.0 → Fixed in version 650 2.2.0.13
7.	Relion 650 series version 2.2.1 → Fixed in version 650 2.2.1.6
8.	Relion SAM600-IO version 2.2.1 → Fixed in version SAM600-IO 2.2.1.6

\* New update in Revision B of this cybersecurity advisory

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 an industrial control network from attacks that originate from outside the network. Such practices include that protection, control & automation 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. Protection, control & automation 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. Block all non-trusted IP communications.

The impact of the vulnerabilities above can be greatly reduced by implementing a firewall to restrict external network connectivity to the affected devices.

## Frequently Asked Questions

### What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could affect communication on the Control Network.

### What causes the vulnerability?

The vulnerability is caused by insufficient input data validation in the TCP/IP stack in VxWorks used in some ABB Grid Automation products.

### What is VxWorks and what is the TCP/IP stack?

VxWorks is the real time operating system used by some ABB Grid Automation products. It includes e.g. the TCP/IP stack which is the SW component handling the network communication. IPNet is the name of the TCP/IP stack used in the affected product version.

### What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could disrupt ongoing communication or block new communication on the Control Network

### How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating specially crafted messages and sending the message to an affected controller. For some of the messages this would require that the attacker has direct access to the Control Network. For others the attack could additionally also be done through a wrongly configured or penetrated firewall. An attack could also be done by installing malicious software on a system node or otherwise infect 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?

These corrections remove the vulnerability by applying security updates from Wind River that modify the way that the TCP/IP stack validates messages. The controller's network security protection measures are also extended

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

The list of vulnerabilities in VxWorks has been publicly disclosed by Wind River. Hitachi ABB Power Grids advisories are published here: <https://www.hitachiabb-powergrids.com/cybersecurity/alerts-and-notifications>.

### When this security advisory was issued, had ABB 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.

## References

Information from Wind River about the VxWorks vulnerabilities is available here:

<https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/>

## Acknowledgement

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

Wind River for providing patches and remediation recommendations to address the vulnerabilities present in their software.

## 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/>.

## Revision

Date	Revision	Description
2021-03-08	A	1 <sup>st</sup> version of the cybersecurity advisory
2021-05-19	B	Update on Recommended Immediate Actions Section <ul style="list-style-type: none"><li>Relion 650 series version 1.3.0 → Fixed in revision 650 1.3.0.7</li></ul> Fix broken links. Update to Hitachi ABB Power Grids template.