CyberSecurity Advisory for IPNET
Vulnerabilities

ABBVU-PGGA-Relion670-1MRG035814
ABBVU-PGGA-Relion650-1MRG035815
ABBVU-PGGA-SAM600-IO-1MRG035816

Notice

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

ABB 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 ABB 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 ABB 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 ABB, 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.

© Copyright 2020 ABB. All rights reserved.
Affected Products

<table>
<thead>
<tr>
<th>Products and Affected Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Relion 670 series version 2.2.0.9 through version 2.2.0.12</td>
</tr>
<tr>
<td>2. Relion 670 series version 2.2.1.0 through version 2.2.1.5</td>
</tr>
<tr>
<td>3. Relion 670 series version 2.2.2.0 and version 2.2.2.2</td>
</tr>
<tr>
<td>4. Relion 670 series version 2.2.3.0 and version 2.2.3.1</td>
</tr>
<tr>
<td>5. Relion 650 series version 1.3.0.0 through version 1.3.0.6</td>
</tr>
<tr>
<td>6. Relion 650 series version 2.2.0.9 through version 2.2.0.12</td>
</tr>
<tr>
<td>7. Relion 650 series version 2.2.1.0 through version 2.2.1.5</td>
</tr>
<tr>
<td>8. Relion SAM600-IO version 2.2.1.0 through version 2.2.1.4</td>
</tr>
</tbody>
</table>

Vulnerability ID

ABB ID: ABBVU-PGGA-Relion670-1MRG035814
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 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public. Relion 670/650/SAM-IO series is affected by these vulnerabilities.

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 Link: https://www.first.org/cvss/calculator/[

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 Link: https://www.first.org/cvss/calculator/[

CVE-2019-12259 DoS via NULL dereference in IGMP parsing
CVSS v3 Base Score: 7.5
CVSS v3 Temporal Score: 6.7
CVSS v3 Link: https://www.first.org/cvss/calculator/[

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 Link: https://www.first.org/cvss/calculator/[

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
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 Link: https://www.first.org/cvss/calculator/...

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 Link: https://www.first.org/cvss/calculator/...

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 Link: https://www.first.org/cvss/calculator/...

Vulnerability Details

Relion 670/650/SAM600-IO product uses the TCP/IP stack from the operating system VxWorks. A 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.

CVE-2019-12256: 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.

CVE-2019-12258: 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.

CVE-2019-12260: 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.

**CVE-2019-12261** 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.

**CVE-2019-12263** 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.

**CVE-2019-12259**: DoS via NULL dereference in IGMP parsing
By sending specially crafted IGMP packets, an attacker could potentially trigger a Denial-of-Service condition.

**CVE-2019-12262** 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.

**CVE-2019-12265** 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 actions**

ABB is preparing to provide maintenance releases to address these vulnerabilities in all affected products.

The issue is corrected in the following product versions:

<table>
<thead>
<tr>
<th>Products and Fixed Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Relion 670 series version 2.2.0 → Fixed in version 670 2.2.0.13</td>
</tr>
<tr>
<td>2. Relion 670 series version 2.2.1 → Fixed in version 670 2.2.1.6</td>
</tr>
<tr>
<td>3. Relion 670 series version 2.2.2 → Fixed in version 670 2.2.2.3</td>
</tr>
<tr>
<td>4. Relion 670 series version 2.2.3 → Fixed in version 670 2.2.3.2</td>
</tr>
<tr>
<td>5. Relion 650 series version 1.3.0 → Planned</td>
</tr>
<tr>
<td>6. Relion 650 series version 2.2.0 → Fixed in version 650 2.2.0.13</td>
</tr>
<tr>
<td>7. Relion 650 series version 2.2.1 → Fixed in version 650 2.2.1.6</td>
</tr>
<tr>
<td>8. Relion SAM600-IO version 2.2.1 → Fixed in version SAM600-IO 2.2.1.6</td>
</tr>
</tbody>
</table>
ABB recommends that customers apply the update at the earliest convenience.

**Mitigating 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**

1. **What is the impact on my system?**
   This depends on the system setup. In many cases the system impact is low because we have a gateway in place which separates the communication from extern network to the internal networks in different zones. There is no direct communication through the gateway possible.

2. **When will be maintenance release available?**
   ABB is working on the maintenance release for the affected products. After we have verified the maintenance release we will publish this on the extern web page: ABB Cyber Security portal

3. **What is ABB’s recommendation?**
   ABB recommends adding an external firewall and to implement ACL (Access Control List) so that our system communicates only with trusted parties.
   The implementation of VPN will also make sure that you communicate only with trusted parties.

4. **Is there a workaround until the maintenance release is available?**
   Yes, implement 3rd party firewalls using ACL or implement VPN communication between the substation and the control center.

5. **Who can help me to install and configure the firewall?**
   Please contact your local ABB organization. They can help you to analyses and implement cyber security measures.

6. **Where do I get a firewall?**
   Please contact your local ABB organization. They can offer you a industrial firewall suitable for your
7. How do I implement ACL (Access Control List) in the firewall?  
   How to configure the ACL is documented in the firewall user manual.  
   Your local ABB unit can support you in reviewing the current firewall setting and implementing the  
   required ACL (Access Control List) for your control system.

References

Information from WindRiver about the VxWorks vulnerabilities is available here:  

Acknowledgements

ABB thanks the following for working with us to help protect customers:  
Wind River for providing patches and remediation recommendations to address the vulnerabilities pre-

Support

For additional information and support please contact your local ABB service organization. For contact  
information, see https://new.abb.com/contact-centers.  
Information about ABB’s cyber security program and capabilities can be found at  
www.abb.com/cybersecurity.