ABB

CYBER SECURITY ADVISORY

WindRiver VxWorks IPNet Vulnerabilities, impact on ETL600 Power Line Carrier System
ABBVU-PGGA-ETL600-1KHW003576

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

Products and Affected Versions
- ETL600, LAN module R1LB version 1.02 through version 1.07

Vulnerability ID

ABB ID: ABBVU-PGGA-ETL600-1KHW003576

CVE ID: CVE-2019-12255, CVE-2019-12258, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263

Summary

On the 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public. ETL600 is affected by some of these vulnerabilities, which are listed above.

An attacker who successfully exploits these vulnerabilities could 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-2019-12255   TCP Urgent Point = 0 leads to integer underflow

CVSS v3 Base Score: 9.8

CVSS v3 Temporal Score: 9.8

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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 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: 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

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

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

Vulnerability Details

The ETL600 LAN moduel R1LB uses the TCP/IP stack from the operating system VxWorks. The vulnerabilities that exist in the VxWorks operating system are included in the product versions listed above. An attacker who successfully exploits these vulnerabilities could hijack existing TCP sessions to inject packets of their choosing or cause Denial of Service (DoS) attacks.

CVE-2019-12255: TCP Urgent Point = 0 leads to integer underflow
An attacker can either highjack an existing TCP-session and inject bad TCP-segments or establish a new TCP-session on any TCP-port the victim system listens to. Most likely outcome is a crash of the application reading from the affected socket. In the worst case, this vulnerability can potentially lead to remote code execution

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-2019-12261 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-2019-12262 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-2019-12263 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.

Recommended immediate actions

The issue is corrected in the following product version:

Products and Fixed Versions
- ETL600 R4.2.3, LAN module R1LB v1.08

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 net-work 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.

Workarounds

If an update of the devices is not possible for the operator, a workaround is to restrict access to the devices to only trusted parties/devices.

Frequently Asked Questions

1. **What is the scope of the vulnerability?**

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

2. **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.

3. **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.

4. **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

5. **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.

6. **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.

7. **What does the update do?**

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

8. **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. ABB has published the Cyber Security Notification at https://new.abb.com/about/technology/cyber-security/alerts-and-notifications .

9. **When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?**

    No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

References

Information from WindRiver about the VxWorks vulnerabilities is available here:

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

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 present in their software.

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.