PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory 02/2019

VxWorks RPC Buffer Overflow Vulnerability (CVE-2019-9865)

Document Version: 1.0
Release Date: 18th of September, 2019

Notice

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

B&R 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 B&R 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 B&R 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 B&R, 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 © 2019 B&R. All rights reserved.

1. Vulnerability Information

Vulnerability Title: VxWorks RPC Buffer Overflow Vulnerability

CVE number: CVE-2019-9865

CVSS v3 Score: 8.1

Affected software: VxWorks

Affected software versions: 6.6 to 6.9

Fixed (not affected) software versions: 6.9.1 and above

Software manufacturer: Wind River

Vulnerability Description

Vulnerable software component: VxWorks RPC service

Vulnerability trigger: Specially crafted RPC requests sent to vulnerable devices

Potential attack impacts on affected devices:

- Execution of arbitrary code
- Denial of service

Further details about this vulnerability are available on various websites linked in section 4.

Vulnerability relevance for B&R Products

Automation Runtime (“AR”) software running on various B&R devices is based on VxWorks.
As a consequence, the AR versions listed below are affected by this vulnerability.

Copyright © B&R

2. Affected B&R Products

Affected product: Automation Runtime

Affected product versions:

- 4.00 to 4.05

B&R products running the software versions mentioned above are affected by this vulnerability.

3. B&R Action Plan

Wind River does not provide a patch for the VxWorks version used in affected AR versions.
As a consequence, B&R cannot provide a patch for affected AR versions which closes this vulnerability.

Customers using affected AR versions are encouraged to

- take safeguarding measures to minimize risks arising from exploitation of this vulnerability as outlined below
- consider upgrading their AR devices to the current/most recent AR version

Copyright © B&R

4. Safeguarding Measures/Mitigations

Customers are strongly advised to take the following measures to minimize risks arising from exploits leveraging this vulnerability:

a. Place industrial control systems (ICS) in a dedicated network containing ICS components only
b. Use firewalls to isolate ICS networks from all other (e.g. business) networks
c. Create strict firewall rules to thoroughly filter network traffic targeting this vulnerability (“exploit traffic”)
d. Optional: Use Intrusion Detection Systems (IDS) to monitor your networks for exploit traffic
e. Optional: Use Intrusion Preventions Systems (IPS) to protect ICS from exploit traffic

Important note:
Please use caution when implementing safeguarding measures. It is your responsibility to make sure such measures do not have side effects interfering with normal ICS operations.

General ICS Security Guidelines

- Locate ICS networks and devices behind firewalls and isolate them from any other networks like business networks and the Internet.

- Block any inbound Internet traffic destined for the ICS network/devices. Place remote access devices used for remote ICS access outside the ICS network.

- Limit outbound Internet traffic originating from ICS devices/networks as much as possible.
  If ICS devices must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which ICS devices definitely need to use for normal ICS operations.
  If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.

- Limit exposure of ICS networks/devices to internal systems. Tailor firewall rules allowing traffic from internal systems to ICS networks/devices to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal ICS operations.

- If supported by your firewall and thoroughly tested in advance, apply additional filters to allowed traffic which provide protection for ICS networks/systems. Such filters are provided by advanced firewall features like IPS (Intrusion Prevention), Application Control and Anti-Virus.

- In case you use an IPS solution, consider using IPS rules protecting against ICS exploits.

- In case you want to filter internal ICS network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.

- Use trusted software, software patches, Anti-Malware programs and interact only with trusted web sites and trusted email attachments.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please note that VPN solutions may have vulnerabilities and should be updated to the most current version available.

- For further support on ICS security measures please contact your IT service provider.

Copyright © B&R

4. Further details and information sources

[1]
Wind River vulnerability information
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-9865

[2]
National Vulnerability Database (NDV) vulnerability information
https://nvd.nist.gov/vuln/detail/CVE-2019-9865

[3]
CVE Details vulnerability information
https://www.cvedetails.com/cve/CVE-2019-9865/

Copyright © B&R