Cyber Security Advisory #03/2021

NAME:WRECK Impact on Automation Runtime and ARwin

Document Version: 1.1

First published: 2021-05-10
Last updated: 2021-06-30

Notice

Executive Summary

CVE-2016-20009 NAME:WRECK Impact on Automation Runtime and ARwin
Forescout Research Labs, partnering with JSOF Research, disclosed NAME:WRECK, a set of Domain Name System (DNS) vulnerabilities that have the potential to cause either Denial of Service (DoS) or Remote Code Execution, allowing attackers to take targeted devices offline or to gain control over them.

The vulnerability could be exploited by an attacker on the same network or on a remote network by spoofing packets.

Affected Products

Details about B&R software versioning schemes are outlined in Automation Studio help page with GUID 51b2a741-a05d-48c1-957c-2aa1ad5cc8d4[1].

The time periods in Table 1 are preliminary and may be subject to change. Registered customers may approach their local B&R service organization in case of questions.

B&R Automation Runtime

B&R Automation Runtime is affected by CVE-2016-20009.

Table 1 lists affected B&R Automation Runtime versions.

Affected Base Versions	Patched Version	Patch Availability
All versions prior to 4.7x	-	-
4.7x	F4.73	October 2021
4.8x	D4.83	October 2021

Table 1: Overview on affected Automation Runtime versions, patched versions, and release dates

B&R Automation Runtime versions >=4.9x are not impacted by CVE-2016-20009.

B&R Automation Runtime ARwin

B&R Automation Runtime ARwin is affected by CVE-2016-20009.

Table 2 lists affected B&R Automation Runtime ARwin versions.

Affected Base Versions	Patched Version	Patch Availability
All versions of ARwin	-	-

Table 2: Overview on affected Automation Runtime ARwin versions, patched versions, and release dates

B&R does not provide patches for affected B&R Automation Runtime ARwin versions.

[1] Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 5.

Vulnerability ID

CVE-2016-20009 NAME:WRECK Impact on Automation Runtime and ARwin

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2016-20009 NAME:WRECK Impact on Automation Runtime and ARwin

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

Corrective Actions or Resolution

B&R recommends applying product updates at the earliest convenience.
Users of Automation Runtime versions 4.6 and prior are advised to upgrade to a newer version.

For users of ARwin, B&R recommends addressing the cyber security risk originating from this security issue by implementing the recommendations in section Workarounds and Mitigations.

Vulnerability Details

CVE-2016-20009 NAME:WRECK Impact on Automation Runtime and ARwin

Description

The vulnerability exists in the TCP/IP stack implementation of the underlying operating system.
A network-based attacker may craft spoofed network packets to exploit a buffer overflow issue in this TCP/IP stack implementation.

Impact

This vulnerability may lead to a Denial of Service (DoS) or arbitrary code execution on affected B&R Automation Runtime versions and B&R Automation Runtime ARwin versions This may allow an adversary to take target component offline or to take over control of the component.

Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations, when patching or upgrading to patched versions is not possible.

It is recommended to configure usage of internal DNS servers only and block external DNS traffic where possible. Furthermore, it is recommended to segment networks and shield affected devices from untrusted networks by using e.g. firewalls.
Network intrusion detection mechanisms may be applied to filter malicious packets[2].

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines.
Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

References

[1] Forescout and JSOF Disclose New DNS Vulnerabilities, Impacting Millions of Enterprise and Consumer Devices

`https://www.forescout.com/research-labs/namewreck/`

[2] NAME:WRECK Breaking and fixing DNS implementations

`https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/`

Document History

Version	Date	Description
1.0	2021-05-10	Initial version
1.1	2021-06-30	Concluded internal impact analysis; conversion to security advisory; added preliminary patch availability

Appendix

Accessing a help page via GUID

To go to a help page using a GUID, do the following in the AS Help Explorer:

- Press Ctrl + G or select View > Goto Page
- Enter the GUID of the help page as shown in the following screenshot: