PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Notice #03/2021

NAME:WRECK - Impact on B&R Products

Document Version: 1.0

First published: 2021-05-10
Last updated: N/A (Initial version)

Executive Summary

On April 12th, 2021, a series of vulnerabilities affecting four TCP/IP stacks, were made public through the Forescout security blog[1]. B&R is aware of these security issues, known as `NAME:WRECK`.

B&R is evaluating the impact for all potentially affected B&R products and has initiated its vulnerability handling process. B&R products, which implement one of the four TCP/IP stacks might be affected by one or more of the Common Vulnerabilities and Exposures (CVEs) listed in Table 1.

The vulnerability CVE numbers and CVSS scores are listed in Table 1.

CVE ID	CVSSv3.1 Score
CVE-2020-7461	7.7
CVE-2016-20009	9.8
CVE-2020-15795	8.1
CVE-2020-27009	8.1
CVE-2020-27736	6.5
CVE-2020-27737	6.5
CVE-2020-27738	6.5
CVE-2021-25677	5.3
TBA[1]	6.5

Table 1: `NAME:WRECK` related CVE numbers and corresponding CVSS score

[1] The security researchers from Forescout Research Labs and JSOF are waiting for a CVE ID to be assigned to this issue.

Affected Products

B&R products named in this section are affected by the `NAME:WRECK` vulnerabilities.

For B&R products not listed in this section the impact analysis is still ongoing.
B&R continues the investigation and updates affected products if they are identified as affected.

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

B&R Automation Runtime

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

Table 2 lists affected B&R Automation Runtime versions.
Information regarding patches for specific affected B&R Automation Runtime versions will be updated in due course of time.

Affected Base Versions	Patched Version	Patch Availability
All versions prior 4.5x	-	-
4.5x	TBA	TBA
4.6x	TBA	TBA
4.7x	TBA	TBA
4.8x	TBA	TBA

Table 2: 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 exclusively by CVE-2016-20009.

Table 3 lists affected B&R Automation Runtime ARwin versions.

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

Table 3: 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.
B&R recommends addressing the cyber security risk originating from this security issue by implementing the recommendations in section Workarounds and Mitigations.

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

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

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: