



## Cyber Security Notice #09/2021

### INFRA:HALT - Impact on B&R Products

Document Version: 1.0

First published: 2021-08-27

Last updated: N/A (Initial version)

#### Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

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.



## Executive Summary

On August 4<sup>th</sup>, 2021, a series of vulnerabilities affecting the NicheStack TCP/IP network stack, were made public through the JFrog's security blog[1]. B&R is aware of these security issues, known as INFRA:HALT. Technical details on these vulnerabilities are documented in a research report published by Forescout Research Labs and JFrog Security Research[2].

B&R has initiated its vulnerability handling process.  
B&R has analyzed its product portfolio, which might be affected by one or more of the Common Vulnerabilities and Exposures (CVEs) listed in Table 1, linked to INFRA:HALT.

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

CVE ID	CVSSv3.1 Score
CVE-2020-25928	9.8
CVE-2021-31226	9.1
CVE-2020-25767	7.5
CVE-2020-25927	8.2
CVE-2021-31227	7.5
CVE-2021-31400	7.5
CVE-2021-31401	7.5
CVE-2020-35683	7.5
CVE-2020-35684	7.5
CVE-2020-35685	7.5
CVE-2020-27565	7.5
CVE-2021-36762	7.5
CVE-2020-25926	4
CVE-2021-31228	4

Table 1: INFRA:HALT related CVE numbers and corresponding CVSS score

The conclusion of this analysis is; B&R's product portfolio is not affected by INFRA:HALT.

## Affected Products

None

## 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] JFrog's and Forescout's publication of INFRA:HALT vulnerabilities in NicheStack TCP/IP network stack

<https://jfrog.com/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/>

### [2] Technical details on the INFRA:HALT vulnerabilities

<https://www.forescout.com/resources/infrahalt-discovering-mitigating-large-scale-ot-vulnerabilities/>



## Document History

Version	Date	Description
1.0	2021-08-27	Initial version