PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

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)

Executive Summary

On August 4th, 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 Forscout'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