Cyber Security Advisory #04/2020

Automation Runtime TFTP Service DoS Vulnerability

Document Version: 1.1

First published: 2020-08-12
Last updated: 2020-09-30

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

CVE-2020-11637 Automation Runtime TFTP Service DoS Vulnerability
A memory leak in the TFTP service in B&R Automation Runtime versions <N4.26, <N4.34, <F4.45, <E4.53, <D4.63, <A4.73 and prior could allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition.

Affected Products

Affected products: Automation Runtime
Affected versions: Please refer to Table 1

Affected Base Versions	Patched Version	Release status
<=4.1x	-	-
4.2x	N4.26	Released: 2020-08-04
4.3x	N4.34	Released: 2020-04-20
4.4x	F4.45	Released: 2020-03-27
4.5x	E4.53	Released: 2020-04-30
4.6x	D4.63	Released: 2020-09-04
4.7x	A4.73	Released: 2020-04-06

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

The time period in Table 1 denoted as planned is preliminary and may be subject to change. Registered customers may approach their local B&R service organization in case of questions.

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

Vulnerability ID

CVE-2020-11637 Automation Runtime TFTP Service DoS Vulnerability

Vulnerability Severity

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

CVE-2020-11637 Automation Runtime TFTP Service DoS Vulnerability
CVSS v3.1 Base Score: 5.8 (Medium)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

Corrective Actions or Resolution

The described vulnerabilities will be fixed in the product versions as listed in Table 1.

B&R recommends applying product updates at the earliest convenience.
Users of Automation Runtime versions 4.10 and prior are advised to upgrade to a newer version.

[1] Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 4.

Vulnerability Details

CVE-2020-11637 Automation Runtime TFTP Service DoS Vulnerability

Description

The affected B&R Automation Runtime versions use an underlying operating system that in turn has a TFTP service implementation. This TFTP service implementation has been found to have a memory management issue, not releasing previously allocated memory. An attacker with the ability to send TFTP requests to the system could exhaust the available system memory by sending specially crafted network packets to the affected service.

Impact

Affected B&R Automation Runtime versions may be abused to continuously consume available memory. This vulnerability may lead to denial of service (DoS) conditions, where interaction is hampered and reliability of services are impacted.

Fix

The memory leak has been fixed at operating system level.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations:
TFTP communication should be restricted to legitimate network partners, using e.g. a sufficient Firewall setup and robust network segmentation.

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/

Document History

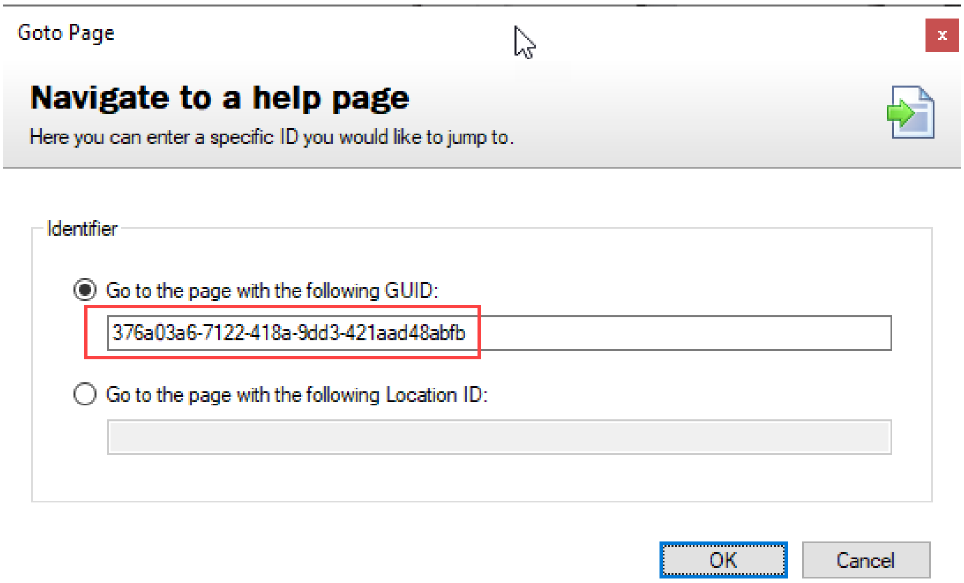
Version	Date	Description
1.0	2020-08-07	Initial version
1.1	2020-09-30	Updated patch availability

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:



Goto Page

Navigate to a help page

Here you can enter a specific ID you would like to jump to.

Identifier

● Go to the page with the following GUID:

376a03a6-7122-418a-9dd3-421aad48abfb

○ Go to the page with the following Location ID: