PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #14/2021

Vulnerabilities in B&R Automation Studio and PVI Windows Services

Document Version: 1.0

First published: 2021-11-30
Last updated: N/A (Initial version)

Notice

Executive Summary

CVE-2020-24681 Automation Studio and PVI Multiple incorrect permission assignments for services
An incorrect permission assignment for B&R Automation Studio and PVI Windows services versions <=4.7.6, <=4.8.5, <=4.9.3 and prior could allow an authenticated local attacker to escalate privileges.

CVE-2020-24682 Automation Studio and PVI Multiple unquoted service path vulnerabilities
An unquoted service path on B&R Automation Studio and PVI Windows services versions <=4.7.6, <=4.8.5, <=4.9.3 and prior could allow an authenticated local attacker to escalate privileges.

Affected Products

Affected products: B&R Automation Studio (AS)
Affected versions: Please refer to Table 1

Affected Base Versions	Patched Version	Release status
<=4.6.x	-	No fix planned
4.7.x	4.7.7 SP	Available
4.8.x	4.8.6 SP	Available
4.9.x	4.9.4 SP	Available

Table 1: Overview on affected, patched versions and release dates on B&R Automation Studio (AS)

Affected products: B&R Automation NET/PVI
Affected versions: Please refer to Table 2

Affected Base Versions	Patched Version	Release status
<=4.6.x	-	No fix planned
4.7.x	4.7.7	Available
4.8.x	4.8.6	Available
4.9.x	4.9.4	Available

Table 2: Overview on affected, patched versions and release dates on B&R Automation NET/PVI

Details about B&R software versioning schemes are outlined in AS help page with GUID 51b2a741-a05d-48c1-957c-2aa1ad5cc8d4 or in chapter Automation software/Version information/Automation Software version overview.[1]

Vulnerability ID

CVE-2020-24681 Automation Studio and PVI Multiple incorrect permission assignments for services
CVE-2020-24682 Automation Studio and PVI Multiple unquoted service path vulnerabilities

[1] Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 6.

Vulnerability Severity

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

CVE-2020-24681 Automation Studio and PVI Multiple incorrect permission assignments for services

CVSS v3 Base Score: 8.2 (High)

CVSS v3 Vector: AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

CVE-2020-24682 Automation Studio and PVI Multiple unquoted service path vulnerabilities

CVSS v3 Base Score: 7.2 (High)

CVSS v3 Vector: AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

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 Studio and PVI versions 4.6 and prior are advised to upgrade to a newer version.

CVE-2020-24681 Automation Studio and PVI Multiple incorrect permission assignments for services

Description

On B&R Automation Studio and PVI the Windows services `BrDiskImageSvcx` and `PviManSvcx` are installed with insufficient permission assignments. An authenticated local attacker could alter these manually started service configurations to escalate privileges.

Impact

Affected B&R Automation Studio and PVI installation may be abused by an authorized but nonprivileged local user to execute arbitrary code with elevated privileges. This affects the confidentiality, integrity and availability of the entire Windows operating system and its data.

Fix

The provided patches reconfigure the B&R Automation Studio and PVI installed Windows services, to allow modification only for privileged users.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.
Users of B&R Automation Studio and PVI may manually reconfigure permission settings on these services to allow modification only for privileged users.
Additionally, it is recommended to limit access to the workstation running B&R Automation Studio and PVI to authorized users.

CVE-2020-24682 Automation Studio and PVI Multiple unquoted service path vulnerabilities

Description

An unquoted service path vulnerability[1] exists in affected B&R Automation Studio and PVI the Windows services `BrDiskImageSvcx` and `PviManSvcx`.
A local authenticated attacker with access to the file system may escalate privileges by inserting arbitrary code into the unquoted service path.

Impact

Users are not affected by this vulnerability if the default installation location has been used.
Affected B&R Automation Studio and PVI installation may be abused by an authorized but nonprivileged local user to execute arbitrary code with elevated privileges. This affects the confidentiality, integrity and availability of the entire Windows operating system and its data.

Fix

The provided patches reconfigure the B&R Automation Studio and PVI installed Windows services preventing

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.
Users of B&R Automation Studio and PVI may manually reconfigure the service paths and enclose them in quotes.
Additionally, it is recommended to limit access to the workstation running B&R Automation Studio and PVI to authorized users.

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/

Acknowledgements

B&R would like to thank the following for working with us to help protect our customers:
Mr. Andrew Hofmans

References

[1] Unquoted Search Path or Element

`https://cwe.mitre.org/data/definitions/428.html`

Document History

Version	Date	Description
1.0	2021-11-30	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: