PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #03/2020

Multiple Vulnerabilities in Automation Studio

Document Version: 1.0

First published: 2020-04-02
Last updated: N/A (Initial version)

Executive Summary

CVE-2019-19100 Privilege escalation via Automation Studio upgrade service
A privilege escalation vulnerability in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, <4.3.11SP, <4.4.9SP, <4.5.4SP, <4.6.3SP, <4.7.2 and <4.8.1 allow authenticated users to delete arbitrary files via an exposed interface.

CVE-2019-19101 Incomplete communication encryption and validation
A missing secure communication definition and an incomplete TLS validation in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, <4.3.11SP, <4.4.9SP, <4.5.5SP, <4.6.4 and <4.7.2 enable unauthenticated users to perform MITM attacks via the B&R upgrade server.

CVE-2019-19102 Zip Slip vulnerability in 3rd-Party library
A directory traversal vulnerability in SharpZipLib used in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x and 4.2.x allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.

Affected Products

Affected products: Automation Studio
Affected versions: Please refer to Table 1.

Vulnerability ID	Affected Automation Studio Version	Patched Version (Release Date)
CVE-2019-19100	4.0.x	-
	4.1.x	-
	4.2.x	-
	<4.3.11SP	4.3.11SP (Planned: 2020-04-16)
	<4.4.9SP	4.4.9SP (Planned: 2020-05-14)
	<4.5.4SP	4.5.4SP (Available)
	<4.6.3SP	4.6.3SP (Available)
	<4.7.2	4.7.2 (Available)
	<4.8.1	4.8.1 (Planned: 2020-04-17)
CVE-2019-19101	4.0.x	-
	4.1.x	-
	4.2.x	-
	<4.3.11SP	4.3.11SP (Planned: 2020-04-16)
	<4.4.9SP	4.4.9SP (Planned: 2020-05-14)
	<4.5.5SP	4.5.5SP (Available)
	<4.6.4	4.6.4 (Available)
	<4.7.2	4.7.2 (Available)
CVE-2019-19102	4.0.x	-
	4.1.x	-
	4.2.x	-

Table 1: Affected versions and scheduled patches

The dates in Table 1 denoted as planned are 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 AS help page with GUID 51b2a741-a05d-48c1-957c-2aa1ad5cc8d4.[1]

[1] Information about how to access a help page with a GUID is provided in section "Accessing a help page via GUID" on page 8.

Vulnerability ID

CVE-2019-19100 Privilege escalation via Automation Studio upgrade service
CVE-2019-19101 Incomplete communication encryption and validation
CVE-2019-19102 Zip Slip vulnerability in 3rd-Party library

Vulnerability Severity

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

CVE-2019-19100 Privilege escalation via Automation Studio upgrade service
CVSS v3 Base Score: 7.5 (High)
CVSS v3 Vector: AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:H

CVE-2019-19101 Incomplete communication encryption and validation
CVSS v3 Base Score: 6.5 (Medium)
CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

CVE-2019-19102 Zip Slip vulnerability in 3rd-Party library
CVSS v3 Base Score: 5.5 (Medium)
CVSS v3 Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

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 4.0.x, 4.1.x and 4.2.x are advised to upgrade to a newer version of Automation Studio.

Vulnerability Details

CVE-2019-19100 Privilege escalation via Automation Studio upgrade service

Description

Automation Studio upgrade service runs with elevated privileges. The upgrade service exposes a local system interface to clean up downloaded upgrade files. This functionality may be abused to induce arbitrary file paths, on which a delete operation will be called.

Impact

An adversary having access to the Windows system on which Automation Studio is installed, may attach to the exposed upgrade service interface to delete arbitrary files from this system.

Fix

The upgrade service now operates with reduced privileges (`NT AUTHORITY\LocalService` [1]). Additionally, the deletion process is restricted to Automation Studio downloaded files and directories.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.
It is possible to manually adjust the permissions of the Automation Studio upgrade service to e.g. `NT AUTHORITY\LocalService` [1]. Access to the Automation Studio installation and the device it's used on should be restricted.

CVE-2019-19101 Incomplete communication encryption and validation

Description

Automation Studio upgrade service fetches configuration files from B&Rs upgrade server. These configuration files contain HTTP links to relevant upgrade files hosted on B&Rs upgrade server. The fetched configuration files and updates are not transmitted via HTTPS.
Additionally, the upgrade service implements an incomplete certificate validation mechanism.

Impact

An attacker in a privileged network position could alter the destination to fetch files from a location under adversary control.

Fix

B&Rs upgrade server now serves HTTPS links in the configuration files. Additionally, Microsoft .NET Framework certificate checks are now being used in the Automation Studio upgrade service.

Workarounds and Mitigations

B&R has not identified any workarounds or mitigating factors for the incomplete certificate validation mechanism in the Automation Studio upgrade service.

CVE-2019-19102 Zip Slip vulnerability in 3rd-Party library

Description

Automation Studio upgrade service versions before 4.3 implement the 3rd-party ZIP archive library SharpZipLib [2].
The library version used is prone to the Zip Slip vulnerability [3], which introduces a directory traversal issue in the upgrade service.

Impact

A malicious entity may abuse the vulnerability e.g. described in CVE-2019-19101 to induce a crafted ZIP archive to then perform an arbitrary write operation.
The vulnerability may not be exploited to overwrite existing files or write to Windows system directories, like `C:\Windows\System32`.

Fix

Automation Studio 4.3 and later switched from SharpZipLib to the .NET Framework provided native ZIP archive implementation. For these versions the issue is not reproducible. For prior version of Automation Studio, it is recommended to update the installation.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.
Access to zip archives is controlled and exposure of the zip archive is limited to trusted parties only.

Checksums may be used to detect tampering of zip archives, e.g. transferring them between different contexts.

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/

Frequently Asked Questions

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, B&R received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had B&R received any reports that this vulnerability was being exploited?

No, B&R had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

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

- Mr. Nadav Erez from Claroty

References

[1] Windows service LocalService User

`https://docs.microsoft.com/en-us/windows/win32/services/localservice-account`

[2] SharpZipLib compression library

`https://github.com/icsharpcode/SharpZipLib`

[3] Zip Slip vulnerability

`https://snyk.io/research/zip-slip-vulnerability`
`https://snyk.io/vuln/SNYK-DOTNET-SHARPZIPLIB-60247`
`https://github.com/icsharpcode/SharpZipLib/issues/232`

Support

For additional information and support, please contact your local B&R service organization. For contact information, see www.br-automation.com.

Document History

Version	Date	Description
1.0	2020-04-02	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: