DOCUMENT ID: SA23P019
VERSION: 1.0
DATE: 2024-02-22

CYBER SECURITY ADVISORY

B&R Automation Studio & Technology Guarding B&R products use insufficient communication encryption

CVE ID: CVE-2024-0220

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

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.

Purpose

B&R has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, B&R immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If B&R is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of B&R's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

- B&R Automation Studio < 4.6
- B&R Technology Guarding < 1.4.0

Vulnerability IDs

CVE-2024-0220

Summary

A fix in the B&R web service interface solves a vulnerability in the product versions listed above.

An insecure communication channel in the Upgrade Service of B&R enables network-based unauthenticated attackers to sniff sensitive data or insert and run arbitrary code.

The support of the insecure communication channel will be disabled on 29th February 2024.

Recommended immediate actions

The problem is corrected on the B&R server-side in the following product versions:

- B&R Automation Studio versions >=4.6
- B&R Technology Guarding versions >= 1.4.0

B&R recommends using B&R Automation Studio >=4.6 and/or B&R Technology Guarding >= 1.4.0 at earliest convenience.

The process to install updates for the affected products is described in the user manual. The step to identify the installed product version is described in the user manual.

Vulnerability severity and details

A vulnerability exists in services hosted by B&R and used by B&R Automation Studio Upgrade Service and B&R Technology Guarding, included in the product versions listed above. A network attacker could exploit the vulnerability by intercepting the network traffic, which allows inserting and running arbitrary code on the products and sniffing sensitive data.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2024-0220 - B&R products use insufficient communication encryption.

B&R Automation Studio Upgrade Service and B&R Technology Guarding use insufficient cryptography for communication to the upgrade and the licensing servers. A network-based attacker could exploit the vulnerability to execute arbitrary code on the products or sniff sensitive data.

CVSS v3.1 Base Score:	8.3 (High)
CVSS v3.1 Temporal Score:	7.2 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-0220

Mitigating factors

Configure a firewall to disable support for TLS <1.2
Customers could configure a firewall to disable support for TLS <1.2 for connections to the B&R servers. Even if the support for TLS <1.2 is disabled on the B&R server-side, a network attacker could emulate an upgrade server that still supports these legacy TLS versions, making the vulnerability still exploitable.

Verification of B&R digitally signed upgrade files
B&R upgrade files are digitally signed, and their signatures are checked by Windows UAC before installation. However, the customers should verify the publisher certificate during the Windows UAC prompt and not only rely on the displayed published name (Microsoft, 2023).

Additionally, refer to section “General security recommendations” for further advise on how to keep your system secure.

[1] The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations’ computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

Workarounds

B&R has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

If the customer wants to continue using Automation Studio < 4.6

Manual upgrade for packages
The customer would not be able to use the Upgrade Service of the B&R Automation Studio anymore. Thus, the customer would need to download the upgrade packages manually from the B&R website.

Usage of B&R Technology Guarding
The customer must upgrade to a later version of B&R Technology Guarding and use B&R Technology Guarding as a standalone application. Thus, the customer can only transfer their license by opening B&R Technology Guarding as a standalone application and not through B&R Automation Studio.

Frequently asked questions

What is the scope of the vulnerability?

A network attacker who successfully exploited this vulnerability could insert and run arbitrary code on an affected product and sniff sensitive data.

What causes the vulnerability?

The vulnerability is caused by using an insecure communication channel in the Upgrade Service in the B&R Automation Studio and in the B&R Technology Guarding.

What is B&R Automation Studio?

B&R Automation Studio is an environment for developing and executing automation solutions, ranging from control and motion technology to HMI, operation, and integrated safety technology.

What is B&R Technology Guarding?

B&R Technology Guarding is a central application installed once on a machine to handle license protection for individual software components. B&R Technology Guarding is part of different B&R product installing packages:

- B&R Automation Studio
- Process Visualization Interface
- AS Target for Simulink
- APROL

What might an attacker use the vulnerability to do?

A network attacker successfully exploiting this vulnerability could insert and run arbitrary code on the products or sniff sensitive data.

How could an attacker exploit the vulnerability?

A network attacker could try to exploit the vulnerability by intercepting and altering the network communication of an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

How is the vulnerability solved?

The B&R server has disabled an insecure communication channel by only allowing HTTPS communication using TLS 1.2 or higher.

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

No, B&R discovered this vulnerability as a part of its own security analyses.

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.

General security recommendations

For any installation of software-related B&R products we strongly recommend the following (non-exhaustive) list of cyber security practices:

Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general purpose network (e.g. office or home networks).

Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.

Never connect programming software or computers containing programing software to any net-work other than the network for the devices that it is intended for.

Scan all data imported into your environment before use to detect potential malware infections.

Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.

Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.

When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

References

Microsoft. (2023, January 6). *How User Account Control works*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/how-it-works

Support

For additional instructions and support please contact your local B&R service organization. For contact information, see https://www.br-automation.com/en/about-us/locations/.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Version history

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date
1.0	all	Initial version	