DOCUMENT ID: ADVISORY_03/2022
VERSION: 1.1
DATE: 2022-12-14

CYBER SECURITY ADVISORY

B&R Technology Guarding Impact of Vulnerability in WIBU CodeMeter Runtime to B&R Products

CVE ID: CVE-2021-41057

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

Affected Products	Versions
B&R Automation Studio (AS)	>=4.0
Process Visualization Interface (PVI)	>=4.0
B&R Technology Guarding (TG)	<=1.3
AS Target for Simulink	>=6.2
APROL	>=R4.0

Vulnerability IDs

CVE-2021-41057

Summary

B&R is aware of public reports of a vulnerability in WIBU systems product CodeMeter Runtime for Windows, which could cause a Denial of Service of systems running this product by overriding existing files.

The vulnerable product is integrated in B&R Technology Guarding, which is part of the B&R products listed above.

Recommended immediate actions

B&R Technology Guarding is a central application installed once on a machine to handle license protection for individual software components. Changing or updating B&R Technology Guarding therefore affects all B&R products on this machine.

B&R Technology Guarding is available as standalone installer and is part of different B&R product installing packages:

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

The problem is fixed in the following product versions:

Product	Patched Versions
B&R Technology Guarding (TG)	1.4.03

B&R Technology Guarding Upgrades are available for downloading on the B&R webpage:

https://www.br-automation.com/en/downloads/software/technology-guarding/technology-guarding/

Follow the described steps through the installation. Verify the installed version by opening the B&R Technology Guarding app and reading the version information in the window title bar.

B&R recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the WIBU CodeMeter Runtime for Windows component included in the product versions listed above. An attacker could exploit the vulnerability by overriding existing files on the affected system, causing a Denial-of-Service condition.

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

CVE-2021-41057 CodeMeter Runtime for Windows: Denial of Service (DoS)

If a local attacker with basic user capabilities is able to set up a link to a special system file, then essential files in the machine running the B&R products listed above could get overwritten. Exploiting the vulnerability requires at least an unprivileged user account on the machine.

CVSS v3.1 Base Score: 7,1
CVSS v3.1 Temporal Score: 6,4

[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.

CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2021-41057

Mitigating factors

If not in use, disabling the container type “Mass Storage” in CodeMeter can mitigate the vulnerability:

If there are no CmDongles connected to the affected machine or if the connected CmDongles are configured as HID, the CodeMeter communication with “Mass Storage” devices can be disabled at the Windows Registry as follows:

Set the value of the key “HKEY_LOCAL_MACHINE\SOFTWARE\WIBUSYSTEMS\CodeMeter\Server\CurrentVersion\EnabledContainerTypes” to 4294967294 (0xFFFFFFFE).

Workarounds

An attacker needs unprivileged local access to exploit the vulnerability. B&R customers are advised to harden systems running affected B&R products, preventing access by untrusted users.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could cause a denial-of-service condition on systems running affected B&R products.

What causes the vulnerability?

The vulnerability is caused by improper file access permission controls in the WIBU CodeMeter Runtime for Windows, which is part of B&R Technology Guarding.

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 local attacker who successfully exploited this vulnerability could cause a crash of the CodeMeter Runtime Server which may lead to denial-of-service condition of the system running the affected B&R product.

How could an attacker exploit the vulnerability?

A local attacker with basic user capabilities could try to exploit the vulnerability by setting up a link to a special system file used with CmDongles.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have local access to an affected system.

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

Yes, this vulnerability has been publicly disclosed.

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 network 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.

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	
1.1	Recommended immediate actions	Patch version is available	2022-12-14