DOCUMENT ID: SA24P005
VERSION: 1.0
DATE: 2024-05-14

CYBER SECURITY ADVISORY

Insecure Loading of Code in B&R Products

CVE ID: CVE-2024-2637

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

Analyzing the products is an ongoing process. The following products have currently been identified as being vulnerable:

Product name	Affected versions
Scene Viewer	< 4.4
Automation Runtime • **Automation Runtime Simulation** • **B&R Hypervisor Installer**	<= I4.93
mapp Vision	< 5.26.1
mapp View	< 5.24.2
mapp Cockpit	< 5.24.2
mapp Safety	< 5.24.2
Visual Components (VC) 4	< 4.73.2

Vulnerability IDs

CVE-2024-2637

Summary

Updates are available that resolve a vulnerability in the product versions listed above.

An authenticated local attacker who successfully exploited this vulnerability could insert and run arbitrary code using legitimate B&R software.

Recommended immediate actions

The problem is corrected in the following product versions:

Product name	Fixed version	Availability
Scene Viewer	4.4.0	Released
Automation Runtime • **Automation Runtime Simulation** • **B&R Hypervisor Installer**	J4.93	Released
mapp Vision	5.26.1	Released
mapp View	5.24.2	Released
mapp Cockpit	5.24.2	Released
mapp Safety	5.24.2	Pending
Visual Components (VC) 4	4.73.2	Released

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

The process to install updates 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 the several B&R software components included in the product versions listed above. An authenticated local attacker could exploit the vulnerability by running arbitrary code using legitimate B&R software.

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

CVE-2024-2637

An uncontrolled search path element vulnerability in several B&R software products could allow an authenticated local attacker to execute malicious code by placing specially crafted files in the loading search path.

CVSS v3.1 Base Score:	7.2 (High)
CVSS v3.1 Temporal Score:	6.9 (Medium)
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-2637

Mitigating factors

Strengthen installation folder permissions

To avoid the replacement of legitimate with malicious DLL, ensure that the B&R software installation folders are only writable by privileged users.

Ensure Safe DLL search mode is enabled

Safe DLL search mode is enabled by default on Windows operating systems. However, there might be scenarios where this is disabled. For more information, please refer to the Microsoft website [1].

Follow least-privilege principles and ensure the physical security of the computers

Ensure that only authorized users have access to the computers and that their privileges are restricted to the minimum necessary (least-privilege principle).

Refer to section “General security recommendations” for further advice on how to keep your system secure.

Frequently asked questions

What is the scope of the vulnerability?

An authenticated local attacker who successfully exploited this vulnerability could insert and run arbitrary code using malicious DLL files and executables on an affected system node.

What causes the vulnerability?

The vulnerability is caused by exploiting the Windows search and load order used by software applications for loading DLL files and improper integrity checks when executing code from untrusted locations.

[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.

What is B&R Scene Viewer

B&R Scene Viewer is a software to visualize the movements of machines in a 3D environment. The animation of the machine components is controlled by cyclically reading OPC-UA watchables, typically from a PLC.

What is B&R Automation Runtime (AR)?

B&R Automation Runtime (AR) is a real-time operating system running on all B&R target systems.

What is VC 4?

B&R VC4 is a software package for generating human-machine interfaces using Automation Studio. These interfaces can be used to control machines or display information about current operations. B&R VC4 visualization is using VNC technology

What is mapp Vision?

Together with B&R's fully integrated vision solution, the mapp Vision software package makes machine vision applications much easier to create, maintain and diagnose.

What is mapp Safety?

mapp Safety allows complete integration of safety technology into the mapp framework, making it easier to create, maintain and diagnose safety applications.

What is mapp View?

With mapp View, automation engineers have all the tools they need to create powerful, intuitive, web-enabled HMI screens. There is no need to deal with the underlying web technology. This technology is encapsulated in widgets, which are simply dragged and dropped into place and configured.

What is mapp Cockpit?

mapp Cockpit provides a convenient single point of access for machine commissioning and diagnostics. Built on web-based mapp View HMI technology, mapp Cockpit works on any hardware platform with a standard browser.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could run arbitrary code using malicious DLL files or executables on an affected system node.

How could an attacker exploit the vulnerability?

An authenticated local attacker can use the Windows search and load order or replace legitimate software components in an insufficient secured system to execute malicious code. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an authenticated 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.

What does the update do?

The updates restrict the search sequence when loading components and limit the execution of components from untrusted sources.

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 is not aware that the vulnerability is being exploited in any of the listed products when this advisory was published.

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.

References

[1] Microsoft, "Dynamic-link library search order," 2 February 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order#search-order-for-unpackaged-apps.

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	14.05.2024