DOCUMENT ID: SA22P014
VERSION: 1.0
DATE: 2024-11-27

CYBER SECURITY ADVISORY

Authentication bypass flaw in several mapp components

CVE ID: CVE-2024-10490

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

Product	Affected Version
mapp Cockpit	5.x
mapp View	5.x
mapp Services	5.x (only if mpUserX or mpCodeBox is used)
mapp Motion	5.x
mapp Vision	5.x

Vulnerability IDs

CVE-2024-10490

Summary

An update is available that resolves a vulnerability in the product versions listed above.

An attacker who successfully exploits this vulnerability may read and change data or cause denial of service conditions.

Recommended immediate actions

B&R recommends that customers perform a risk assessment for their application/IACS and apply the update at earliest convenience or follow the mitigation/workaround guide.

The problem is corrected in the following product versions:

Product	Patched Version
mapp Cockpit	6.0
mapp View	6.0
mapp Services	6.0
mapp Motion	6.0
mapp Vision	6.0

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.

Be aware, that additional steps are necessary after installing the upgrades to configure a proper authentication mechanism and get the products back into operation. Please refer to the individual migration guides of the products for further guidance.

Vulnerability severity and details

Users of the affected products need to explicitly configure access to the OPC UA Server with an insufficiently secure authentication token. During operation the components expose functionality in a hidden format on that interface. An unauthenticated network-based attacker may abuse this functionality by guessing the access procedure.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

CVE-2024-10490

An “Authentication Bypass Using an Alternate Path or Channel” vulnerability in the OPC UA Server configuration required for B&R mapp Cockpit before 6.0, B&R mapp View before 6.0, B&R mapp Services before 6.0, B&R mapp Motion before 6.0 and B&R mapp Vision before 6.0 may be used by an unauthenticated

[1] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

[2] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations’ computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

network-based attacker to cause information disclosure, unintended change of data, or denial of service conditions.

B&R mapp Services is only affected, when mpUserX or mpCodeBox are used in the Automation Studio project.

CVSS v3.1 Base Score:	7.7 (High)
CVSS v3.1 Temporal Score:	6.7 (Medium)
CVSS v3.1 Vector:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/E:U/RL:O/RC:C
CVSS v4.0 Score	8.4 (High)
CVSS v4.0 Vector:	https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-10490

Mitigating factors

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

Workarounds

Enforce client device authentication in the configuration of the OPC UA server. Configure a proper “SecurityPolicy” for OPC-UA Server (Automation Help) and select a “CertificateStore configuration” which has “Validate SSL communication partner” set to “on” (Automation Help).

Limit access to the OPC UA Server (default 4840/tcp) to IP addresses or IP subnets which are running instances of impacted mapp components and legitime OPC UA clients using the B&R Automation Runtime host-based firewall. Ensure only trusted personal is able to access devices with the specified IP (range) and enforce strict authentication on these devices.

Please be aware that B&R Automation Runtime and its services (like mapp components) are not intended to be directly connected to the internet at any time. Customers are advised to use the host-based firewall as well as an external control network firewall to limit access to each service running at B&R Automation Runtime. Additionally, consider granting access from the outside of the control network only to specific timeframes (e.g. for maintenance).

mapp View

For customers only using the OPC UA Server for their mapp View Visualization, block all incoming traffic to the OPC UA Server (default port 4840/tcp) using the B&R Automation Runtime host-based firewall. Blocking external traffic on the OPC UA Server has no impact on the functionality of mapp View.

Frequently asked questions

What causes the vulnerability?

The product requires authentication, but the product has an alternate path or channel that does not require authentication.

What is mapp Cockpit?

mapp Cockpit is a web-based HMI (Human Machine Interface) application that provides functions for diagnostics and commissioning for B&R Automation. It is integrated directly into the web-based mapp Cockpit HMI application and available via function blocks.

What is mapp View?

mapp View is a technology package in B&R Automation's mapp (modular application technology) suite that enables automation engineers to create powerful and intuitive HMI applications without having to deal with underlying web technology. mapp View supports the drag-and-drop placement and configuration of integrated components called "widgets" to cover all functions of a machine's user interface

What is mapp Motion?

mapp Motion is a technology package provided by B&R Automation that includes components for controlling single-axis movements, CNC machines, robots, and transport systems in machine and system applications. With mapp Motion, basic functions are already implemented in the components, making configuration faster and easier.

What is mapp Service?

mapp Services is a technology package provided by B&R Automation for machines. It offers the latest features and components to realize the infrastructure of a machine. mapp Services provides an easy way to create alarm-, recipe-, or user management

What is mapp Vision?

mapp Vision is a technology package provided by B&R Automation that is used for implementing lighting and image capture scenarios in machine and system applications. It offers several functions such as position detection, completeness inspection, quality grading, measurement, and identification. mapp Vision also provides encapsulated algorithms for image processing that are easily configurable and allow a variety of tasks to be solved quickly without having to write a single line of code.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could access functionality provided by the impacted components without proper authentication. This may lead to the disclosure and alteration of information or cause denial of service conditions at IACS by triggering methods and procedures.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to 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.

What does the update do?

The update introduces a secure by default and authenticated access configuration for mapp components to the OPC UA Server of Automation Runtime. Users need to take explicit action to change to an insecure configuration.

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 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.

More information on recommended practices can be in the document Defense in Depth for B&R products.

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	2024-11-27