DOCUMENT ID: SA26P012
VERSION: 1.0
DATE: 2026-09-03

CYBER SECURITY ADVISORY

mapp Services
Use of Weak Authenticators in mapp Audit
CVE ID: CVE-2026-79679

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

mapp Audit used in mapp Services versions < 6.8.0

Vulnerability IDs

CVE-2026-79679

Summary

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

An attacker who successfully exploits this vulnerability could gain access to the OPC UA server component on affected devices due to insufficient entropy of authenticators used by mapp Audit.

Recommended immediate actions

The problem is corrected in the following product versions:

mapp Services >= 6.8.0

B&R recommends that customers apply the update at earliest convenience when the vulnerable functionality mapp Audit is used.

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

Only systems on which the mapp Audit functionality of mapp Services has been explicitly integrated and configured are affected by this vulnerability. Projects that merely include mapp Services are not affected unless mapp Audit is actively used.

When mapp Audit is configured, affected versions rely on authenticators used during operation that do not provide sufficient entropy for access to the OPC UA server functionality. These authenticators are not static, fixed, or publicly documented credentials. An attacker with network access could exploit this weakness to gain access to the OPC UA server functionality used by mapp Audit.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2026-79679

A vulnerability in mapp Audit in B&R mapp Services before version 6.8.0 is caused by insufficient entropy of the authenticators, which could allow an attacker with network access to gain access to the OPC UA server functionality used by mapp Audit.

CVSS

CVSS v3.1 Base Score:	8.7
CVSS v3.1 Temporal Score:	7.6
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/RL:O
CVSS v4.0 Score	7.0
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N

CWE

CWE-1391: Use of Weak Credentials

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-79679

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] 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.

[3] 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.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

Mitigating factors

The exposure is limited to systems that actively use the mapp Audit functionality. Projects that only include mapp Services, but do not configure or use mapp Audit, are not affected. The risk can be further reduced by restricting network access to the affected OPC UA server, for example by limiting access to trusted engineering stations, runtime components, or dedicated automation network segments using the Automation Runtime host-based firewall.

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

Frequently asked questions

What is mapp Services?

With mapp Services, B&R provides modular software components that cover basic functions of machines and systems.

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 removes the vulnerability by increasing the entropy of the authenticators used by mapp Audit.

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

No, B&R discovered the vulnerability through its own security analysis.

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 found in the following documents:

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	2026-09-03