DOCUMENT ID: SA25P001
VERSION: 1.1
DATE: 2025-01-16

CYBER SECURITY ADVISORY

Automation Runtime and mapp View Use of insecure algorithm for self-signed certificates

CVE ID: CVE-2024-8603

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 Runtime <6.1

B&R mapp View < 6.1

Vulnerability IDs

CVE-2024-8603

Summary

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

An attacker who successfully exploited this vulnerability may masquerade as services on affected devices.

Recommended immediate actions

The problem is corrected in the following product versions:

B&R Automation Runtime version 6.1.

B&R mapp View 6.1.

B&R recommends that customers apply the update at their earliest convenience if B&R Automation Runtime or B&R mapp View is used to generate self-signed certificates on production machines.

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

B&R Automation Runtime and B&R mapp View generates self-signed certificates during the boot-up process if no certificates have been configured in the B&R Automation Studio project. These certificates are signed using an algorithm, which is no longer considered to be secure.

Please note that the mechanism of creating self-signed certificates during bootup is only intended for testing and not for real-world environments. In general, the use of self-signed certificates is not aligned with cyber security best practices due to their lack of trust verification.

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-2024-8603

A “Use of a Broken or Risky Cryptographic Algorithm” vulnerability in the SSL/TLS component used in B&R Automation Runtime versions <6.1 and B&R mapp View versions <6.1 may be abused by unauthenticated network-based attackers to masquerade as services on impacted devices.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CVSS v4.0 Score	8.2
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-8603

Mitigating factors

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

Workarounds

The mechanism of creating self-signed certificates on B&R Automation Runtime and B&R mapp View during bootup is only intended for testing and not for production machines. Please use always a proper

[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.

SSL/TLS configuration in B&R Automation Studio including certificates signed by a trusted certificate authority for machines used in production environments.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by the usage of insecure cryptographic algorithms for generating self-signed certificates in B&R Automation Runtime and B&R mapp View.

What is B&R Automation Runtime?

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

What is B&R 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 might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could masquerade as a service on an affected device.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by intercepting the communication between a client an impacted server. 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 removes the vulnerability by changing the used cryptographic algorithm.

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

No, B&R received information about this vulnerability through responsible disclosure.

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	2025-01-15
1.1	P3	Link to NVD	2015-01-16