DOCUMENT ID: SA25P002
VERSION: 1.0
DATE: 2025-10-07

CYBER SECURITY ADVISORY

# B&R Automation Runtime DoS Vulnerability in System Diagnostics Manager (SDM)

CVE ID: CVE-2025-3450

## 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

Automation Runtime version <6.3 and <Q4.93

# Vulnerability IDs

CVE-2025-3450

# Summary

An update is available that resolves a vulnerability identified by B&Rs internal security analysis in the product versions listed above.

An attacker who successfully exploited this vulnerability could cause the product to stop.

# Recommended immediate actions

The problem is corrected in Automation Runtime versions 6.3 and Q4.93.

The System Diagnostic Manager (SDM) is disabled by default in Automation Runtime 6 and is not intended be enabled on active systems located outside properly secured production networks or in facilities lacking adequate physical and logical access controls to prevent any form of unauthorized interaction. For customers who use SDM on their systems, B&R recommends applying the update at the 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 product versions listed above. An attacker could exploit the vulnerability by sending specially crafted messages to the system node, causing the node to stop.

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

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[3].

### CVE-2025-3450 Automation Runtime SDM requests may impact system

An Improper Resource Locking vulnerability in the SDM component of B&R Automation Runtime versions before 6.3 and before Q4.93 may allow an unauthenticated network-based attacker to delete data causing denial of service conditions.

**CVSS**

| | |
|---|---|
| CVSS v3.1 Base Score: | 10.0 |
| CVSS v3.1 Temporal Score: | 8.7 |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E:U/RL:O/RC:C |
| | |
| CVSS v4.0 Score | 9.3 |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H |

**CWE**
CWE-413: Improper Resource Locking

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-3450

# Mitigating factors

**Deactivate the vulnerable component**

The SDM is deactivated by default on Automation Runtime version >=6.0. For Automation Runtime versions <6.0, the SDM can be deactivated in the Automation Studio project. Please refer to Automation Help GUID 1d915d67-07f7-4034-a472-c204b5cabbfe for further guidance.

---

[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.

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

Access to the System Diagnostic Manager (SDM) shall be restricted to trusted personnel through appropriate external security measures. If SDM is required solely for maintenance purposes, it should be enabled or access granted only for the minimum time necessary to perform the task.

**Limit accessibility**

B&R recommends in general to configure the HTTP protocol over TLS (HTTPS).

Customers may restrict access to the webserver by configuring mutual TLS (mTLS) in the Automation Studio project (Option “Validate SSL communication partner”). Be aware that configuring mTLS would impact also other applications using the AR webserver (e.g. mapp View). Please refer to Automation Help GUID 01ced6c0-28ef-4aaa-bd05-2442b971859c to learn more about the TLS Configuration in Automation Studio.

In addition, accessibility of the webserver can be limited to trusted IP addresses using the Automation Runtime host-based firewall. Please refer to Automation Help GUID 75b8994b-f97a-4e0f-8278-43c7a737e65f for details.

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

# Frequently asked questions

### What causes the vulnerability?

The vulnerabilities are caused by improper resource locking.

### What is System Diagnostics Manager (SDM)?

System Diagnostics Manager (SDM) is a webpage available over the Automation Runtime Webserver, showing key diagnostic information of the running controller

### What is Automation Runtime (AR)?

B&R Automation Runtime is a middleware system enabling customers to run applications on B&R target systems.

### What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could cause the affected system node to stop.

### 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.

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

No, B&R discovered the vulnerabilities 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 net-work 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 | 2025-10-07 |
| | | | |
| | | | |