DOCUMENT ID: SA25P003
VERSION: 1.0
DATE: 2025-10-07

CYBER SECURITY ADVISORY

B&R Automation Runtime Vulnerabilities in System Diagnostic Manager (SDM)

CVE ID: CVE-2025-3449, CVE-2025-3448

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 < 6.4

Vulnerability IDs

CVE-2025-3449, CVE-2025-3448

Summary

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

An attacker who successfully exploited these vulnerabilities could take over a remote session or execute code in the context of the user's browser session.

Recommended immediate actions

The problem is corrected in Automation Runtime 6.4.

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 based on risk assessment 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

Security vulnerabilities have been identified in the SDM component of the affected product versions listed above. These flaws could be exploited by an attacker either through successful prediction of a user's session ID or by deceiving the user into clicking a maliciously crafted hyperlink.

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-2025-3449 Weak Session Token used in Automation Runtime SDM

A Generation of Predictable Numbers or Identifiers vulnerability in the SDM component of B&R Automation Runtime versions before 6.4 may allow an unauthenticated network-based attacker to take over already established sessions.

CVSS

CVSS v3.1 Base Score:	4.2
CVSS v3.1 Temporal Score:	3.9
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:F/RL:O/RC:C
CVSS v4.0 Score	2.3
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

CWE

CWE-340: Generation of Predictable Numbers or Identifiers

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-3449

CVE-2025-3448 - XSS on SDM

Reflected cross-site scripting (XSS) vulnerabilities exist in System Diagnostics Manager (SDM) of B&R Automation Runtime versions before 6.4 that enables a remote attacker to execute arbitrary JavaScript code in the context of the attacked user's browser session

---

[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/.

CVSS

CVSS v3.1 Base Score:	6.1
CVSS v3.1 Temporal Score:	6.0
CVSS v3.1 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:F/RC:C
CVSS v4.0 Score	5.1
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CWE
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-3448

Mitigating factors

Do not enable the System Diagnostics Manager when it is not required

Refer to section “Frequently asked questions

What causes the vulnerabilities?

The vulnerabilities are caused by insufficient input sanitization and generation of predictable numbers.

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 vulnerabilities to do?

An attacker who successfully exploited these vulnerabilities could cause to run arbitrary code in the context of the user’s browser session or take over the user’s session. Since the SDM currently does not process any session-specific data and also does not implement authentication mechanisms at the session level, B&R is not aware of any advantages an attacker could gain by taking over the session ID.

How could an attacker exploit the vulnerabilities?

To exploit the XSS vulnerability CVE-2025-3448, an attacker could try to create a hyperlink including malicious script code. This hyperlink must be opened by the user to launch the attack.

To exploit vulnerability CVE-2025-3449, an attacker would need to guess a user's session ID.

Could the vulnerabilities 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 further advise on how to keep your system secure.

Workarounds

Do not use Hyperlinks provided by untrusted 3rd party to access the SDM. Hyperlinks may be provided via:

- Emails from unknown users
- Social media channels
- Messaging services
- Webpages with comment functionality
- QR Codes

The use of external Web Application Firewalls (WAF) can mitigate attacks using reflected cross-site scripting.

Frequently asked questions

What causes the vulnerabilities?

The vulnerabilities are caused by insufficient input sanitization and generation of predictable numbers.

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 vulnerabilities to do?

An attacker who successfully exploited these vulnerabilities could cause to run arbitrary code in the context of the user's browser session or take over the user's session. Since the SDM currently does not process any session-specific data and also does not implement authentication mechanisms at the session level, B&R is not aware of any advantages an attacker could gain by taking over the session ID.

How could an attacker exploit the vulnerabilities?

To exploit the XSS vulnerability CVE-2025-3448, an attacker could try to create a hyperlink including malicious script code. This hyperlink must be opened by the user to launch the attack.

To exploit vulnerability CVE-2025-3449, an attacker would need to guess a user's session ID.

Could the vulnerabilities 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 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	2025-10-07