DOCUMENT ID: SA22P024
VERSION: 1.0
DATE: 2023-02-14

CYBER SECURITY ADVISORY

Automation Runtime
Reflected Cross-Site Scripting Vulnerabilities in SDM

CVE ID: CVE-2022-4286

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.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

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

All B&R Automation Runtime (AR) versions >=3.00 and <=C4.93

Vulnerability IDs

CVE-2022-4286

Summary

B&R is aware of serval reflected cross-site scripting vulnerabilities in the System Diagnostics Manager (SDM) component of Automation Runtime versions >=3.00 and <=C4.93.

An attacker could use the vulnerability to construct a hyperlink that, if issued by another user, will cause to execute malicious script code within the user's browser in the context of the user's session.

Recommended immediate actions

The problem is corrected in the following product versions:

B&R Automation Runtime version >=D4.93

B&R recommends that customers apply the update at 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 System Diagnostics Manager included in the product versions listed above. An attacker could exploit the vulnerability by creating a hyperlink including malicious script code, which could lead to remote code execution in the context of the attacked user's browser session. An attacker who successfully exploited this vulnerability could modify or steal information available in the context of the attacked user's browser session.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2022-4286

A reflected cross-site scripting (XSS) vulnerability exists in System Diagnostics Manager of B&R Automation Runtime versions >=3.00 and <=C4.93 that enables a remote attacker to execute arbitrary JavaScript code in the context of the attacked user's browser session.

CVSS v3.1 Base Score:	6.1
CVSS v3.1 Temporal Score:	6.0
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:F/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-4286

Mitigating factors

Deactivate the System Diagnostics Manager when not needed.

Refer to section "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.

[1] 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.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could insert and run arbitrary Script code in the context of the attacked user’s browser session.

What causes the vulnerability?

The vulnerability is caused by improper input validation in the System Diagnostics Manager of B&R Automation Runtime.

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 B&R Automation Runtime (AR)?

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

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could modify or steal information available in the context of the attacked user’s browser session.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a hyperlink including malicious script code. This hyperlink must be opened by the user to launch the attack.

Could the vulnerability be exploited remotely?

Yes, an attacker does not need physical access to the system running B&R Automation Runtime or to the user's computer.

What does the update do?

The update removes the vulnerability by modifying the way that the System Diagnostics Manager validates input and answers after receiving invalid messages.

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.

Acknowledgement

B&R thanks Steffen Robertz and Gerhard Hechenberger (discovery, analysis, coordination) from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues and working with us as we addressed them.
B&R thanks ABB Device Security Assurance Center for reporting these issues.

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	2023-02-14