DOCUMENT ID: SA23P013
VERSION: 1.0
DATE: 2023-07-26

CYBER SECURITY ADVISORY

B&R Automation Runtime
SYN Flooding Vulnerability in Portmapper

CVE ID: CVE-2023-3242

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

B&R Automation Runtime versions <G4.93

Vulnerability IDs

CVE-2023-3242

Summary

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

An unauthenticated network-based attacker who successfully exploited this vulnerability could cause several services of the system node to get inaccessible.

Recommended immediate actions

The problem is corrected in the following product versions:

Automation Runtime >=G4.93

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 Portmapper service included in the product versions listed above. An attacker could exploit the vulnerability by sending a high number of SYN requests to the system node, causing the node to become inaccessible.

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

CVE-2023-3242

The Portmapper service used in Automation Runtime versions <G4.93 is vulnerable to SYN flooding attacks. An unauthenticated network-based attacker may use this vulnerability to cause several services running on B&R Automation Runtime to become permanently inaccessible.

CVSS v3.1 Base Score:	8.6
CVSS v3.1 Temporal Score:	8.0
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-3242

Mitigating factors

This vulnerability can be mitigated on network level, by limiting the network traffic to the control network, where Automation Runtime systems are intended to be used. Please refer to Level 1 of the Reference Architecture[2].

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

Workarounds

Portmapper is only needed for NFSv2 client on B&R Automation Runtime.

If NFSv2 is not in use, block access to port 111/tcp using the B&R Automation Runtime host-based firewall.

If NFSv2 is in use, limit access to trusted ip addresses or subnets only, using the B&R Automation Runtime host-based firewall.

Due to insufficient security capabilities of NFSv2, B&R discontinued the support of NFSv2 Client in Automation Runtime versions >=G4.93. B&R recommends using protocols like CIFS, FTPS or other protocols with security capabilities for data transfer.

It is also recommended to configure the Automation Runtime as a file transfer client, rather than a file server. This also reduces the attack surface on Automation Runtime.

[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.

[2] https://search.abb.com/library/Download.aspx?DocumentID=9AKK107992A6181&LanguageCode=en&Action=Launch

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could prevent legitimate access to an affected system node.

What causes the vulnerability?

The vulnerability is caused by an improper initialization implementation and insufficient limiting/throttling in the Portmapper service used in B&R Automation Runtime.

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 might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to become inaccessible.

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.

What does the update do?

The update removes the vulnerable Portmapper service from B&R Automation Runtime. Customers using the insecure NFSv2 technology are advised to switch to a data transfer technology offering security capabilities (e. g. CIF, FTPS, …).

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 ABB Device Security Assurance Center for reporting this issue.

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	