DOCUMENT ID: SA23P011
VERSION: 1.1
DATE: 2023-08-09

CYBER SECURITY ADVISORY

B&R APROL
Abuse SLP based traffic for amplification attack

CVE ID: CVE-2023-29552

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 APROL<=4.2-07

Vulnerability IDs

CVE-2023-29552

Summary

Updates are available that resolve a vulnerability in the product versions listed above.

An unauthenticated network-based attacker who successfully exploits this vulnerability could use affected products to cause 3rd party components to become temporarily inaccessible.

Recommended immediate actions

The problem is corrected in B&R APROL versions >= R 4.2-07 with AutoYaST >=4.2-070.0.230605. 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 SLP service included in the product versions listed in section Affected products. An unauthenticated network-based attacker could exploit the vulnerability using spoofed UDP traffic to cause Denial-of-Service conditions on 3rd party devices.

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

CVE-2023-29552

The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker to register arbitrary services. This could allow the attacker to use spoofed UDP traffic to conduct a Denial-of-Service attack with a significant amplification.

CVSS v3.1 Base Score:	8.6
CVSS v3.1 Temporal Score:	8.6
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-29552

Mitigating factors

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

Workarounds

SLP is not required for standard operation of APROL. B&R recommends deactivating the SLP service and removing the openslp package if not required:

1. As root „`systemctl stop slpd; systemctl disable slpd; systemctl mask slpd`”
2. As root “`rpm -e –nodeps openslp-server`”

If SLP service is required for normal operation of the Industrial Automation and Control System (IACS), use the host-based firewall and the network-level firewall to restrict access to the port offering the SLP service (default 427). Grant access only the specific IP addresses or trusted network segments.

If SLP service is only required for commissioning or maintenance, additionally block network traffic to the service except defined time frames using policies or deactivate service manually after completing the required activities.

[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 unauthenticated network-based attacker who successfully exploit this vulnerability could conduct a Denial-of-Service attack with a significant amplification.

What causes the vulnerability?

The vulnerability is caused by allowing unauthenticated user to register arbitrary services on the SLP service used in B&R APROL.

What is B&R APROL?

APROL is an Industrial Automation and Control System (IACS), which was developed as a homogeneous, integrated complete system. Central engineering with a global engineering database allows completely consistent automation.

What might an attacker use the vulnerability to do?

An unauthenticated network-based attacker who successfully exploit this vulnerability could cause 3rd party components to stop or become inaccessible.

How could an attacker exploit the vulnerability?

An attacker may exploit the vulnerability by registering arbitrary services on the SLP service of 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 the attacker 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 SLP service.

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

Yes, this vulnerability has been publicly disclosed.

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.

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	2023-05-31
1.1	p2	Updated corrected versions	2023-08-09