

CYBER SECURITY ADVISORY

APROL

Impact of PHP2Shell

CVE ID: CVE-2026-109618, CVE-2026-109619

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 / ABB APROL <= R 4.4-65

Vulnerability IDs

CVE-2026-109618, CVE-2026-109619

Summary

B&R is aware of public reports of vulnerabilities in the product versions listed above.

An attacker who successfully exploits these vulnerabilities may insert and run arbitrary code on affected devices.

Recommended immediate actions

B&R is actively working on patch versions for affected products. Based on current planning, these are expected to be released on October 26, 2026 (R 4.4-65) and October 29, 2026 (R 4.4-01). B&R will update this advisory if these dates change.

APROL is intended to be operated only in environments with restricted logical and physical access, as described in the product documentation and in "Defense in Depth for B&R products". Until patches are available and installed, B&R recommends that customers restrict HTTP(S) traffic to the APROL system, particularly from untrusted networks, and implement additional security measures to limit access to the product to trusted personnel. We advise customers to review and validate their current access

restrictions to confirm that logical and physical access controls are configured in line with these recommendations. These measures reduce, but may not fully eliminate, the risk of exploitation.

Vulnerability severity and details

Two vulnerabilities exist in the PHP component included in the product versions listed above. An attacker could exploit the vulnerabilities by sending specially crafted messages to the system node, causing remote code execution.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)¹ for both v3.1² and v4.0³.

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list⁴.

CVE-2026-109618

PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).

CVSS

CVSS v3.1 Base Score: 9.8

CVSS v3.1 Temporal Score: 9.8

CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score 9.2

CVSS v4.0 Vector: **CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N**

CWE

CWE-1325: Improperly Controlled Sequential Memory Allocation

CWE-416: Use After Free

CWE-755: Improper Handling of Exceptional Conditions

CWE-824: Access of Uninitialized Pointer

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/>.

CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/cve-2026-109618>

CVE-2026-109619

PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).

CVSS

CVSS v3.1 Base Score: 9.8

CVSS v3.1 Temporal Score: 9.8

CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score: 9.2

CVSS v4.0 Vector: **CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N**

CWE

CWE-1325: Improperly Controlled Sequential Memory Allocation

CWE-416: Use After Free

CWE-755: Improper Handling of Exceptional Conditions

CWE-824: Access of Uninitialized Pointer

CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/cve-2026-109619>

Mitigating factors

APROL is intended to be operated only in environments with restricted logical and physical access, as described in the product documentation and in “Defense in Depth for B&R products”. Until patches are available and installed, B&R recommends that customers implement additional security measures to limit access to the product to trusted personnel. We advise customers to review and validate their current access restrictions to confirm that logical and physical access controls are configured in line with these recommendations. These measures reduce, but may not fully eliminate, the risk of exploitation.

It is recommended to block any HTTP(S) traffic, particularly from untrusted networks, reaching the APROL system on your connected firewalls.

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

Frequently asked questions

How could an attacker exploit the vulnerabilities?

An attacker could try to exploit the vulnerabilities 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 vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities. 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 these vulnerabilities been publicly disclosed?

Yes, these vulnerabilities have been publicly disclosed.

When this security advisory was issued, had B&R received any reports that these vulnerabilities were being exploited?

No, B&R had not received any information indicating that these vulnerabilities had been exploited in APROL 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 programming 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/cyber-security.

Version history

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date
1.0	all	Initial version	2026-10-23