DOCUMENT ID: SA24P006
VERSION: 1.0
DATE: 2024-04-10

CYBER SECURITY ADVISORY

B&R APROL
Several vulnerabilities in the Docker Engine
CVE IDs: CVE-2024-23652, CVE-2024-21626, CVE-2024-23651, CVE-2024-23653, CVE-2024-23650

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

Product	Affected Versions
B&R APROL R4.2	<= R4.2-07 (SLES 12)
B&R APROL R4.4	<= R4.4-00P2 (SLES 15)

Vulnerability IDs

CVE-2024-23652, CVE-2024-21626, CVE-2024-23651, CVE-2024-23653, CVE-2024-23650

Summary

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

A local attacker who successfully exploited these vulnerabilities could take control of the product by inserting and running arbitrary code into specific Docker Engine components.

Recommended immediate actions

The problem is corrected in the following product versions:

Product	Patched version
B&R APROL R4.2	AutoYaST 4.2-070.0.240402
B&R APROL R4.4	AutoYaST 4.4-001.0.240327

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

Some vulnerabilities exist in the Docker Engine included in the product versions listed above. A local attacker who successfully exploited these vulnerabilities could take control of the product by inserting and running arbitrary code into specific Docker Engine components.

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

CVE-2024-23652

BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit frontend or Dockerfile using RUN --mount could trick the feature that removes empty files created for the mountpoints into removing a file outside the container, from the host system. The issue has been fixed in v0.12.5. Workarounds include avoiding using BuildKit frontends from an untrusted source or building an untrusted Dockerfile containing RUN --mount feature.

CVSS v3.1 Base Score: 6.7 (Medium)
CVSS v3.1 Temporal Score: 5.8 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-23652

CVE-2024-21626

runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc 1.1.11 and earlier, due to an internal file descriptor leak, an attacker could cause a newly-spawned container process (from runc exec) to have a working directory in the host filesystem namespace, allowing for a container escape by giving access to the host filesystem ("attack 2"). The same attack could be used by a malicious image to allow a container process to gain access to the host filesystem through runc run ("attack 1"). Variants of attacks 1 and 2 could be also be used to overwrite semi-arbitrary host binaries, allowing for complete container escapes ("attack 3a" and "attack 3b"). runc 1.1.12 includes patches for this issue.

CVSS v3.1 Base Score: 8.6 (High)
CVSS v3.1 Temporal Score: 7.5 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

[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.

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-21626

CVE-2024-23651

BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. Two malicious build steps running in parallel sharing the same cache mounts with subpaths could cause a race condition that can lead to files from the host system being accessible to the build container. The issue has been fixed in v0.12.5. Workarounds include, avoiding using BuildKit frontend from an untrusted source or building an untrusted Dockerfile containing cache mounts with --mount=type=cache,source=... options.

CVSS v3.1 Base Score: 7.4 (High)
CVSS v3.1 Temporal Score: 6.4 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-23651

CVE-2024-23653

BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. In addition to running containers as build steps, BuildKit also provides APIs for running interactive containers based on built images. It was possible to use these APIs to ask BuildKit to run a container with elevated privileges. Normally, running such containers is only allowed if special `security.insecure` entitlement is enabled both by buildkitd configuration and allowed by the user initializing the build request. The issue has been fixed in v0.12.5 . Avoid using BuildKit frontends from untrusted sources.

CVSS v3.1 Base Score: 7.0 (High)
CVSS v3.1 Temporal Score: 6.1 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-23653

CVE-2024-23650

BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit client or frontend could craft a request that could lead to BuildKit daemon crashing with a panic. The issue has been fixed in v0.12.5. As a workaround, avoid using BuildKit frontends from untrusted sources.

CVSS v3.1 Base Score: 6.2 (Medium)
CVSS v3.1 Temporal Score: 5.4 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-23650

Mitigating factors

General mitigations

Avoid building container images using "docker build" on APROL control computers, especially when building on untrusted base images or using untrusted Dockerfiles (Containerfiles) as input.

If using R4.4-00 or higher consider using "podman build" as an alternative.

In R4.2-07 consider disabling the docker build kit features if container image builds are required.

Restrict the ability to build container images or run containers using docker as much as possible.

If JasperReports Server is installed on the system

Ensure that only the 'aprol-containers-jrs' user is part of the docker group which is allowed to run containers.

If custom workloads are run using docker containers on an APROL control computer and especially if container images are built on the APROL system, follow mitigation steps outlined in the Docker security advisory [1].

If JasperReports Server is not installed on the system

Ensure that the docker service is disabled if no custom containers run on a control computer. If docker is used for custom workloads in R4.4-00 or higher consider using podman and running rootless containers as an unprivileged user as an alternative.

Ensure that the docker group - if it exists - is empty or contains only trusted users, that need the ability to run container workloads.

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

Frequently asked questions

What is the scope of the vulnerabilities?

A local attacker who successfully exploited these vulnerabilities could take control of the product by inserting and running arbitrary code into specific Docker Engine components.

What causes the vulnerabilities?

The vulnerabilities are caused by unchecked input data and improper race conditions in the BuildKit and runc in the Docker Engine part of B&R APROL.

What is B&R APROL?

B&R APROL is an industrial control system, 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 vulnerabilities to do?

A local attacker who successfully exploited these vulnerabilities could take control of the system node and allow the attacker to insert and run arbitrary code.

How could an attacker exploit the vulnerabilities?

An attacker could try to exploit the vulnerabilities by creating a specially crafted Dockerfile and build it on affected system nodes. This would require that the attacker has local access to the system node. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerabilities be exploited remotely?

No, to exploit these vulnerabilities an attacker would need to have physical access to an affected system node.

What does the update do?

The update removes the vulnerabilities by modifying the way that the BuildKit and run verify input data.

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 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 net-work 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.

References

[1] G. Georgieva, "Docker Security Advisory: Multiple Vulnerabilities in runc, BuildKit, and Moby," 31 January 2024. [Online]. Available: https://www.docker.com/blog/docker-security-advisory-multiple-vulnerabilities-in-runc-buildkit-and-moby/.

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	