DOCUMENT ID: SA24P004
VERSION: 1.0
DATE: 2024-02-14

CYBER SECURITY ADVISORY

B&R APROL
SSH service vulnerable to Terrapin attack
CVE ID: CVE-2023-48795

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

The following B&R APROL versions are affected:

Version Line	Version
APROL R 4.2 (SLE12)	<= 4.2-07
APROL R 4.4 (SLE15)	<= 4.4-00

Vulnerability IDs

CVE-2023-48795

Summary

B&R is aware of public reports of a vulnerability in the product versions listed above. An update is available for B&R APROL R 4.4 that resolves a publicly reported vulnerability in the product versions listed above. B&R APROL R 4.2 is in "Classical" phase but for its underlying operating system (SLE12 SP3) the Long Term Service Pack Support (LTSS) for security patches has already ended, thus no patch is published for this vulnerability. We recommend upgrade to APROL R 4.4.

Recommended immediate actions

The problem is corrected in the following product versions:

Version Line	Version
APROL R 4.2 (SLE12)	Long Term Service Pack Support (LTSS) for security patches of SLE 12 SP3 has already ended, thus no patch is published for this vulnerability. It is recommended to upgrade to APROL R 4.4
APROL R 4.4 (SLE15)	APROL-AutoYaST-DVD-V4.4-000.0.240108-SLE15-SP4

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.

APROL R 4.4 is backwards-compatible with APROL R 4.2, however the following protocols and drivers are disabled in the newer version [1]:

- INA
- losXfer
- WDPF

Vulnerability severity and details

A vulnerability exists in B&R APROL version. An attacker, with Man-in-the-Middle capabilities, could manipulate SSH messages and compromise the integrity of connections.

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

CVE-2023-48795 - SSH v2 protocol Terrapin Attack

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms.

CVSS v3.1 Base Score:	5.9
CVSS v3.1 Temporal Score:	5.3
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-48795

[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.

Mitigating factors

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

Workarounds

B&R has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

Disable weak cryptographic schemes

The support for chacha20-poly1305@openssh.com cipher and "encrypt then mac" MACs can be disabled as follow [2]:

- For the openssh server side: In the config file /etc/ssh/sshd_config :
  - If there is a Ciphers line, add *-chacha20-poly1305@openssh.com* to the end of the line. If not, add a new Ciphers line *Ciphers -chacha20-poly1305@openssh.com*
  - If there is a MACs line, add *-*etm** to the end of the line. If not, add a new MACs line *MACs -*etm**
- For the openssh client side: Use the /etc/ssh/ssh_config file with same approach described above.

Frequently asked questions

What is the scope of the vulnerability?

An attacker, with Man-in-the-Middle capabilities, could manipulate SSH messages and compromise the security of connections using ChaCha20-Poly1305 or CBC with Encrypt-then-MAC modes.

What causes the vulnerability?

The vulnerability is caused by improper handling of the handshake phase and the use of sequence numbers by SSH Binary Packet Protocol (BPP) in the SSH service of the 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 vulnerability to do?

An attacker who successfully exploited this vulnerability could manipulate SSH messages and compromise the security of connections using ChaCha20-Poly1305 or CBC with Encrypt-then-MAC modes.

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 vulnerability by improving the way that the B&R APROL SSH service is encrypting the communication.

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 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] B&R Industrial Automation, A3 - Upgrade notes - Installing the APROL system (APROL R4.4).

[2] SUSE Support, "Security Vulnerability: CVE-2023-48795 SSH prefix truncation attack (aka Terrapin Attack)," 18 December 2023. [Online]. Available: https://www.suse.com/support/kb/doc/?id=000021295.

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	