DOCUMENT ID: SA24P011
VERSION: 1.1
DATE: 2024-08-30

CYBER SECURITY ADVISORY

B&R Automation Runtime
Several vulnerabilities in B&R Automation Runtime

CVE IDs: CVE-2020-28895, CVE-2020-1971, CVE-2021-23840, CVE-2021-23841, CVE-2024-5800, CVE-2024-5801

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

B&R Automation Runtime < 6.0.

Vulnerability IDs

CVE-2020-28895, CVE-2020-1971, CVE-2021-23840, CVE-2021-23841, CVE-2024-5800, CVE-2024-5801

Summary

An available update resolves privately and publicly reported vulnerabilities in the product versions listed above.

A network-based attacker who successfully exploits these vulnerabilities could make the product inaccessible, decrypt communication, or inject IP-based traffic into another network segment.

Recommended immediate actions

The problem is corrected in the following product versions:

- B&R Automation Runtime 6.0.2

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 FTP server and VxWorks OS in the product versions listed above. A network attacker who successfully exploits these vulnerabilities could make the product inaccessible by exploiting vulnerable components of VxWorks OS, decrypting communications between the FTP server and a connected FTP client, or injecting IP-based traffic into other network segments.

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

CVE-2020-28895

In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.

CVSS v3.1 Base Score:	7.3 (High)
CVSS v3.1 Temporal Score:	6.4 (Medium)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C
CVSS v4.0 Score	6.9 (Medium)
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2020-28895

CVE-2020-1971

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack.

CVSS v3.1 Base Score:	5.9 (Medium)
CVSS v3.1 Temporal Score:	5.7 (Medium)

[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.

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

CVSS v4.0 Score 8.2 (High)
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-1971

CVE-2021-23840

Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash.

CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Temporal Score: 6.5 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C

CVSS v4.0 Score 8.2 (High)
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-23840

CVE-2021-23841

The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources.

CVSS v3.1 Base Score: 5.9 (Medium)
CVSS v3.1 Temporal Score: 5.2 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C

CVSS v4.0 Score 8.2 (High)
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-23841

CVE-2024-5801

Enabled IP Forwarding feature in B&R Automation Runtime versions before 6.0.2 may allow remote attackers to compromise network security by routing IP-based packets through the host, potentially bypassing firewall, router, or NAC filtering.

CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Temporal Score: 5.7 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C

CVSS v4.0 Score 5.3 (Medium)

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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-5801

CVE-2024-5800

Diffie-Hellman groups with insufficient strength are used in the SSL/TLS stack of B&R Automation Runtime versions before 6.0.2, allowing a network attacker to decrypt the SSL/TLS communication.

CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Temporal Score: 5.7 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N/E:U/RL:O/RC:C

CVSS v4.0 Score 8.3 (High)
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-5800

Mitigating factors

Using the host-based firewall

To prevent packets from being forwarded to other subnet segments (CVE-2024-5801), use the host-based firewall of B&R Automation Runtime and block all traffic except packets with destination IP address of the Ethernet port of the B&R Automation Runtime device.

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

Frequently asked questions

What causes the vulnerabilities?

CVE	Vulnerability cause
CVE-2020-28895	Out-of-bounds write Integer overflow or wraparound
CVE-2020-1971	NULL pointer dereferences
CVE-2021-23840	Integer overflow or wraparound
CVE-2021-23841	NULL pointer dereferences
CVE-2024-5801	Initialization of a resource with an insecure default configuration. Improper isolation or compartmentalization.
CVE-2024-5800	Inadequate encryption strength

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?

A network-based attacker who successfully exploits these vulnerabilities could make the product inaccessible, decrypt communications, or inject packets into another network segment.

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.

What does the update do?

The update removes the vulnerability by implementing OpenSSL official patches, disabling insecure cipher suites, and disabling IP forwarding by default.

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

CVE	Public disclosure
CVE-2020-28895 **CVE-2020-1971** **CVE-2021-23840** **CVE-2021-23841**	Yes, the vulnerability has been publicly disclosed.
CVE-2024-5801 **CVE-2024-5800**	No, B&R discovered this vulnerability as a part of its own security analyses.

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 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	2024-08-09
1.1	p3-5	CVSS scoring and hyperlinks typos fixing	2024-08-30