DOCUMENT ID: SA23P002
VERSION: 1.0
DATE: 2023-04-14

CYBER SECURITY ADVISORY

Several Issues in B&R VC4 Visualization

CVE ID: CVE-2019-8277, CVE-2018-20748, CVE-2023-1617

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 VC4 visualization versions are affected:

Version Line	Version
<3.9*	<=3.96.7
4.0*	<=4.06.4
4.1*	<=4.16.3
4.2*	<=4.26.8
4.3*	<=4.34.6
4.4*	<=4.45.1
4.5*	<=4.53.0
4.7*	<=4.72.9

Prior version lines are also affected.

Vulnerability IDs

CVE-2019-8277, CVE-2018-20748, CVE-2023-1617

Summary

Updates are available that resolve several vulnerabilities in the product versions listed above.

An unauthenticated network-based attacker who successfully exploits these vulnerabilities could bypass the authentication mechanism of the VC4 visualization, read stack memory or execute code on an affected device.

Recommended immediate actions

The problems are corrected in the following product versions:

Version Line	Update Version
<3.9*	discontinued
3.9*	3.96.8
4.0*	Please upgrade to next fixed version line
4.1*	Please upgrade to next fixed version line
4.2*	Please upgrade to next fixed version line
4.3*	4.34.7
4.4*	Please upgrade to next fixed version line
4.5*	Please upgrade to next fixed version line
4.7*	4.73.0

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

Several vulnerabilities exist in the product versions listed above.

An unauthenticated network-based attacker who successfully exploits these vulnerabilities may bypass the authentication mechanism of the VC4 visualization, read stack memory or execute arbitrary code.

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

[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.

CVE-2019-8277

VNC contains multiple memory leaks in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with other vulnerabilities, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	6.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-8277

CVE-2018-20748

VNC contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/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-2018-20748

CVE-2023-1617

Improper authentication mechanism in the VNC server component used by affected B&R VC4 visualizations versions may allow an unauthenticated network-based attacker to bypass the authentication mechanism of the VC4 visualization on affected devices. The impact of this vulnerability depends on the functionality provided in the visualization.

Product users are advised to calculate the CVSS v3.1 Environmental Score. Depending on the offered VC4 visualization functionality, the impact may decrease.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	9.4
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-1617

Mitigating factors

Follow the least functionality principle:

- Do not activate VNC server when not necessary for the operation of the IACS.
- Limit functionality of your human machine interface to the essential minimum.

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 limiting known attack vectors:

- Limit the access to the port running VNC server to trusted network segments or specific IP-addresses using the B&R Automation Runtime host-based firewall.
- Limit the physical access to system nodes running VC4 visualizations to trusted personnel.
- Limit network access to system nodes running VC4 visualizations by using a proper configured control network firewall.
- Use Intrusion Detection Systems to detect unintended connection requests to the system node running the VNC server.

Frequently asked questions

What is the scope of the vulnerabilities?

CVE-2019-8277

An unauthenticated network-based attacker could use this vulnerability to read data from the stack memory on affected devices.

CVE-2018-20748

An unauthenticated network-based attacker could use this vulnerability to execute code on affected devices.

CVE-2023-1617

An unauthenticated network-based attacker could use this vulnerability to bypass the authentication mechanism of the VC4 visualization running on affected devices.

What causes the vulnerabilities?

CVE-2019-8277, CVE-2018-20748

The vulnerabilities are caused by insufficient handling of data in the VNC server used by B&R VC4 visualization.

CVE-2023-1617

The vulnerability is caused by an insufficient authentication mechanism of the VNC server used by B&R VC4 visualization.

What is B&R VC4 visualization?

B&R VC4 is a software package for generating human machine interfaces using Automation Studio. These interfaces can be used to control machines or display information about current operations. B&R VC4 visualization is using VNC technology.

What might an attacker use the vulnerabilities to do?

CVE-2019-8277

An attacker could use this vulnerability for information disclosure.

CVE-2018-20748

An attacker could exploit this vulnerability to execute code on affected devices, which could lead to information disclosure, change of data or denial of service conditions.

CVE-2023-1617

The impact of this vulnerability depends on the functionality provided in the visualization. VC4 applications displaying e. g. process data in a read-only mode may not be abused by this vulnerability impacting the integrity or availability of the system.

In cases where VC4 applications control system states or alter process data, this vulnerability might be abused to stop, change parameters, or read system data of the affected system.

B&R recommends calculating the CVSS v3.1 Environmental Score generating an actionable severity rating for the customer use case.

How could an attacker exploit the vulnerabilities?

CVE-2019-8277, CVE-2018-20748

An attacker could try to exploit these vulnerabilities by creating specially crafting VNC packages and sending them to an affected device.

CVE-2023-1617

An attacker could try to exploit the vulnerability by creating login requests and sending the request to an affected system node or use this type of login requests to get access using a visualization panel connected to an affected system node.

To exploit the vulnerabilities remotely, 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. Alternatively, an attacker requires to have physical access to visualization panels used to configure and control the operation of the machine. 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 vulnerabilities by modifying the authentication algorithm and data handling algorithm in the VNC server used by B&R VC4 visualizations.

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

CVE-2019-8277, CVE-2018-20748

Yes, these vulnerabilities have been publicly disclosed.

CVE-2023-1617

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 was being exploited?

No, B&R had not received any information indicating that these vulnerabilities have 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	2023-04-14