DOCUMENT ID: SA22P011
VERSION: 1.0
DATE: 2023-02-27

CYBER SECURITY ADVISORY

Vulnerable TigerVNC Version used in B&R Products

CVE ID: CVE-2019-15691, CVE-2019-15692, CVE-2019-15693, CVE-2019-15694, CVE-2019-15695

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
Mobile Panel 7100 5MP7120.*	5SWVIS.VC52-ENG all versions
Mobile Panel 7100 5MP7140.*	5SWVIS.MP46-ENG < 3.0.1
Mobile Panel 7100 MP7150.*	5SWVIS.MP47-ENG < 3.01
Power Panel C50	<1.2.0
Power Panel C80	<1.2.0
Power Panel T30	<1.6.0
Power Panel T50	<1.6.0
Power Panel T50 mobile	<1.6.0
Power Panel FT50	<1.6.0
Power Panel T80	<1.6.0

Vulnerability IDs

CVE-2019-15691, CVE-2019-15692, CVE-2019-15693, CVE-2019-15694, CVE-2019-15695

Summary

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

A network-based attacker who successfully exploits these vulnerabilities could possibly insert and run arbitrary code.

Recommended immediate actions

The problems are corrected in the following product versions:

Product	Patch Version	Release
Mobile Panel 7100 5MP7120.*	-	Discontinued
Mobile Panel 7100 5MP7140.*	5SWVIS.MP46-ENG 3.0.1	Released
Mobile Panel 7100 MP7150.*	5SWVIS.MP47-ENG 3.01	Released
Power Panel C50	1.2.0	In Progress
Power Panel C80	1.2.0	In Progress
Power Panel T30	1.6.2	Released
Power Panel T50	1.6.1	Released
Power Panel T50 mobile	1.6.0	Released
Power Panel FT50	1.6.1	In Progress
Power Panel T80	1.6.0	Released

B&R recommends that customers apply the updates 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 TigerVNC included in the product versions listed above. A network-based attacker could exploit these vulnerabilities by sending a specially crafted message to the system node, which may lead to execution of arbitrary code on the affected product.

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-2019-15691

TigerVNC version prior to 1.10.1 is vulnerable to stack use-after-return, which occurs due to incorrect usage of stack memory in ZRLEDecoder. If decoding routine would throw an exception, ZRLEDecoder may try to access stack variable, which has been already freed during the process of stack unwinding. Exploitation of this vulnerability could potentially result into remote code execution.

CVSS v3.1 Base Score: 7.2
CVSS v3.1 Temporal Score: 6.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RL:O
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-15691

CVE-2019-15692

TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow. Vulnerability could be triggered from CopyRectDecoder due to incorrect value checks. Exploitation of this vulnerability could potentially result into remote code execution.

CVSS v3.1 Base Score: 7.2
CVSS v3.1 Temporal Score: 6.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RL:O
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-15692

CVE-2019-15693

TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which occurs in TightDecoder::FilterGradient. Exploitation of this vulnerability could potentially result into remote code execution.

CVSS v3.1 Base Score: 7.2
CVSS v3.1 Temporal Score: 6.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RL:O
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-15693

CVE-2019-15694

TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which could be triggered from DecodeManager::decodeRect. Vulnerability occurs due to the signedness error in processing MemOutStream. Exploitation of this vulnerability could potentially result into remote code execution.

CVSS v3.1 Base Score: 7.2
CVSS v3.1 Temporal Score: 6.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RL:O
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-15694

CVE-2019-15695

TigerVNC version prior to 1.10.1 is vulnerable to stack buffer overflow, which could be triggered from CMsgReader::readSetCursor. This vulnerability occurs due to insufficient sanitization of PixelFormat. Since remote attacker can choose offset from start of the buffer to start writing his values, exploitation of this vulnerability could potentially result into remote code execution.

CVSS v3.1 Base Score: 7.2

CVSS v3.1 Temporal Score: 6.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RL:O
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-15695

Mitigating factors

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

Workarounds

To exploit the vulnerabilities, a network-based attacker must get an affected product to connect to the attacker’s server. Secure the network containing VNC clients and servers, so no foreign nodes can pretend to be a VNC server e. g. using spoofing technics.

Frequently asked questions

What is the scope of the vulnerabilities?

An attacker who successfully exploits these vulnerabilities could insert and run arbitrary code in an affected system node.

What causes the vulnerabilities?

The vulnerabilities are caused by insufficient data validation in TigerVNC used in the products listed above.

What might an attacker use the vulnerabilities to do?

An attacker who successfully exploits these vulnerabilities may be able to insert and run arbitrary code on an affected B&R product.

How could an attacker exploit the vulnerabilities?

To exploit these vulnerabilities, an attacker needs to place a specially prepared VNC server in a network containing affected B&R products and get the VNC clients to connect to the malicious VNC server.

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 applies a patched version of TigerVNC to the B&R products.

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

Yes, these vulnerabilities have been publicly disclosed for the affected 3rd party component.

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 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	2022-02-27