DOCUMENT ID: SA24P002
VERSION: 1.1
DATE: 2024-04-12

CYBER SECURITY ADVISORY

Impact of LogoFail vulnerability on B&R Industrial PCs and HMI products

CVE IDs: CVE-2023-5058, CVE-2023-39538, CVE-2023-39539, CVE-2023-40238

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
APC2100	<= 1.44
APC2200	<=1.33
APC3100	<=1.43
APC4100	< 1.06
APC910	<= 1.25
C80	<=1.13
MPC2100	<= 1.44
MPC3100	<=1.22
PPC1200	<=1.13
PPC2200	<=1.33
PPC3100	<=1.43
PPC900	<= 2.13

Vulnerability IDs

CVE-2023-5058, CVE-2023-39538, CVE-2023-39539, CVE-2023-40238

Summary

B&R is aware of public reports of some vulnerabilities in third-party components used by the product versions listed above. An update is available that resolves some publicly reported vulnerabilities in the product versions listed above.

An attacker who successfully exploits these vulnerabilities could make the product inoperable or insert and run arbitrary code at the most sensitive stage of the boot process, which is known as DXE, short for Driver Execution Environment.

Recommended immediate actions

Product	Applicable CVE	Patch Version	Release/Remarks
APC2100	CVE-2023-5058	-	Not exploitable, as the functionality to change the logo is not present.
APC2200	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
APC3100	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
APC4100	CVE-2023-40238	1.06	Released
APC910	CVE-2023-39538	-	Not impacted.
C80	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
MPC3100	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
PPC1200	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
PPC2100	CVE-2023-5058	-	Not exploitable, as the functionality to change the logo is not present.
PPC2200	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.

Product	Applicable CVE	Patch Version	Release/Remarks
PPC3100	CVE-2023-40238	-	Not exploitable, as only JPG/JPEG image types are supported for B&R BIOS versions.
PPC900	CVE-2023-39538	-	Not impacted.

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.

Vulnerabilities severity and details

A series of vulnerabilities exist in the BIOS versions included in the product versions listed above. An attacker who successfully exploits these vulnerabilities would make the product inoperable or insert and run arbitrary code at the most sensitive stage of the boot process, known as DXE, short for Driver Execution Environment.

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

CVE-2023-5058 - Improper Input Validation in the processing of user-supplied splash screen during system boot in Phoenix SecureCore™ Technology™ 4

Improper Input Validation in the processing of user-supplied splash screen during system boot in Phoenix SecureCore™ Technology™ 4 potentially allows denial-of-service attacks or arbitrary code execution.

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.0
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-5058

CVE-2023-39538 - Improper Input Validation of BMP Logo files in AMI AptioV

AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a BMP Logo file with dangerous type by Local access. A successful exploit of this vulnerability may lead to a loss of Confidentiality, Integrity, and/or Availability.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 6.7
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-39538

[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-2023-39539 - Improper Input Validation of PNG Logo files in AMI AptioV

AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a PNG Logo file with dangerous type by Local access. A successful exploit of this vulnerability may lead to a loss of Confidentiality, Integrity, and/or Availability.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-39539

CVE-2023-40238 - Improper Input Validation of BMP Logo files in Insyde InsydeH2O

A LogoFAIL issue was discovered in BmpDecoderDxe in Insyde InsydeH2O with kernel 5.2 before 05.28.47, 5.3 before 05.37.47, 5.4 before 05.45.47, 5.5 before 05.53.47, and 5.6 before 05.60.47 for certain Lenovo devices. Image parsing of crafted BMP logo files can copy data to a specific address during the DXE phase of UEFI execution. This occurs because of an integer signedness error involving PixelHeight and PixelWidth during RLE4/RLE8 compression.

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	5.0
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-40238

Mitigating factors

B&R ensures that the functionality of changing the BIOS logo is only accessible to trusted personnel and only JPG images are used as logos.

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?

An attacker who successfully exploits these vulnerabilities could cause an affected system node to stop or insert and run arbitrary code on an affected system node.

What causes the vulnerabilities?

Vulnerabilities are caused by usage of vulnerable BIOS firmware from a third-party vendor.

What is a B&R Industrial PC?

A B&R industrial PC (IPC) is designed for use in industrial environments and is built to handle more demanding conditions than a standard PC. They often feature robust construction, resistance to dust and moisture, extended temperature ranges, and other specifications suited for industrial applications.

What is B&R C80?

The B&R Power Panel C80 is a combination of a powerful controller with a modern operator terminal into one HMI device, streamlining automation and control processes. It features robust construction, resistance to dust and moisture, extended temperature ranges, and other specifications suited for industrial applications.

What is BIOS?

BIOS, which stands for Basic Input/Output System, is software that is embedded in a computer's motherboard, and it is a part of the booting process of a computer.

What might an attacker use the vulnerabilities to do?

An attacker who successfully exploits these vulnerabilities could cause the affected system node to stop or become inaccessible 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 PNG or BMP image to be used as a booting logo using the BIOS interface. 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 BIOS verifies 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.

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	11.04.2024
1.1	p3-5	Added new products. Explanations improvements and corrections.	12.04.2024