CYBER SECURITY ADVISORY

B&R PCs vulnerable to PixieFail attack

CVE ID: CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237

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
APC4100	< 1.09
APC910	>= 1.25
C80	< 1.14
MPC3100	< 1.24
PPC1200	< 1.14
PPC900	< 2.16
APC2200	< 1.35
PPC2200	< 1.35
APC3100	< 1.45
PPC3100	< 1.45

Vulnerability IDs

CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237

Summary

An update is available that resolves some publicly reported vulnerabilities in the product versions listed above.

A network attacker could exploit the vulnerabilities to execute remote code, initiate DoS attacks, conduct DNS cache poisoning, or extract sensitive information.

Recommended immediate actions

The problems are corrected in the following product versions:

Product	Patch Version	Remarks
APC4100	1.09	
APC910	No patch will be released.	Please refer to the mitigation measures specified in this advisory.
C80	1.14	
MPC3100	1.24	
PPC1200	1.14	
PPC900	2.16	
APC2200	1.35	
PPC2200	1.35	
APC3100	1.45	
PPC3100	1.45	

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

Vulnerabilities exist in the UEFI (Unified Extensible Firmware Interface) firmware included in the product versions listed above. A network attacker could exploit the vulnerabilities to execute remote code, initiate DoS attacks, conduct DNS cache poisoning, or extract sensitive information.

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

CVE-2023-45229 - Integer underflow when processing IA_NA/IA_TA options in a DHCPv6 Advertise message

EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing the IA_NA or IA_TA option in a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	5.9
CVSS v3.1 Vector:	CVSS:3.1/AV:A/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-2023-45229
CWE:	CWE-125 - Out-of-Bounds Read

CVE-2023-45230 - Buffer overflow in the DHCPv6 client via a long Server ID option

EDK2's Network Package is susceptible to a buffer overflow vulnerability via a long server ID option in DHCPv6 client. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.

CVSS v3.1 Base Score:	8.3
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-45230
CWE:	CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2023-45231 - Out-of-bounds read when handling a ND Redirect message with truncated options

EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing Neighbor Discovery Redirect message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	5.9
CVSS v3.1 Vector:	CVSS:3.1/AV:A/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-2023-45231
CWE:	CWE-125 - Out-of-Bounds Read

CVE-2023-45232 - Infinite loop when parsing unknown options in the Destination Options header

EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing unknown options in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.

CVSS v3.1 Base Score:	7.5

[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 Temporal Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/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-2023-45232
CWE:	CWE-835 - Loop with Unreachable Exit Condition (Infinite Loop)

CVE-2023-45233 - Infinite loop when parsing a PadN option in the Destination Options header

EDK2's Network Package is susceptible to an infinite lop vulnerability when parsing a PadN option in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/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-2023-45233
CWE:	CWE-835 - Loop with Unreachable Exit Condition (Infinite Loop)

CVE-2023-45234 - Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

EDK2's Network Package is susceptible to a buffer overflow vulnerability when processing DNS Servers option from a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.

CVSS v3.1 Base Score:	8.3
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-45234
CWE:	CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2023-45235 - Buffer overflow when handling Server ID option from a DHCPv6 proxy Advertise message

EDK2's Network Package is susceptible to a buffer overflow vulnerability when handling Server ID option from a DHCPv6 proxy Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.

CVSS v3.1 Base Score:	8.3
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-45235
CWE:	CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2023-45236 - Predictable TCP Initial Sequence Numbers

EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.

CVSS v3.1 Base Score:	5.8
CVSS v3.1 Temporal Score:	5.2
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-45236
CWE: CWE-338 - Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

CVE-2023-45237 - Use of a weak pseudorandom number

EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.

CVSS v3.1 Base Score: 5.3
CVSS v3.1 Temporal Score: 4.8
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-45237
CWE: CWE-338 - Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Mitigating factors

Deactivate the vulnerable component

The vulnerabilities exist in the Preboot eXecution Environment (PXE) of the UEFI firmware. If this functionality is not needed, it is recommended to disable it in the UEFI settings, thus making the vulnerabilities not exploitable.

Please note, PXE is disabled on default.

Limit accessibility

If PXE functionality is required, users should tightly restrict network traffic to legitimate users and block illegitimate PXE traffic, specifically related to IPv6. For instance, by blocking IPv6 network traffic on the control network firewall.

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?

A network attacker who successfully exploited these vulnerabilities to execute remote code, initiate DoS attacks, conduct DNS cache poisoning, or extract sensitive information. In worst case, these vulnerabilities can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.

What causes the vulnerabilities?

The vulnerabilities are caused by usage of vulnerable UEFI firmware in some B&R xPCs.

What is a B&R xPC?

A B&R xPC is an industrial PC (IPC) 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 might an attacker use the vulnerabilities to do?

A network attacker who successfully exploited the vulnerabilities could execute remote code, initiate DoS attacks, conduct DNS cache poisoning, or extract sensitive information.

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 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 vulnerabilities in the TCP/IP stack used by the UEFI firmware.

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 this vulnerability was being exploited on B&R products?

No, B&R had not received any information indicating that this vulnerability had been exploited on B&R products 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	-
1.1	-	Added description, that PXE is deactivated by default. Added CWE to all CVEs	-
1.2	P2	Corrected affected product version of APC910 to >= 1.25	2026-02-23