CYBER SECURITY ADVISORY

Impact of Insyde UEFI Boot Issues on B&R Products

CVE ID: CVE-2020-27339, CVE-2020-5953, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069

Notice

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 type	Product generation	Affected version
APC	APC 3100	<1.40
	APC 2200	<1.30
PPC	PPC 3100	<1.40
	PPC 2200	<1.30
	PPC 1200	<1.05
	PPC 80	<1.12
MPC	MPC 3100	<1.20

Vulnerability IDs

CVE-2020-27339, CVE-2020-5953, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069

Summary

In February 2022 security researchers at Binarly identified 23 memory management vulnerabilities in Insyde's InsydeH2O UEFI firmware.

These vulnerabilities may be exploited by a privileged authenticated local adversary executing malicious code on affected devices.

The impacted B&R product versions are listed above.

Recommended immediate actions

The problem is corrected in the following product versions:

Product type	Product generation	Bugfix version	Release
APC	APC 3100*	1.40	Released
	APC 2200	1.32	Released
PPC	PPC 3100*	1.40	Released
	PPC 2200	1.32	Released
	PPC 1200	1.05	Released
	PPC 80	1.12	Released
MPC	MPC 3100*	1.21	Released

B&R recommends that customers apply the update at earliest convenience.

The process to install updates is described in the user manual.

*) Please note that BIOS backup/restore function will not work during applying this patch to products APC 3100, PPC3100 and MPC3100. Please refer to Readme.txt of the update for details.

Vulnerability severity and details

Several vulnerabilities exist in InsydeH2O UEFI firmware, included in the product versions listed above. Among these vulnerabilities, the most serious ones could lead to arbitrary code execution or a denial of service condition.

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-2020-27339

In the kernel in Insyde InsydeH2O 5.x, certain SMM drivers did not correctly validate the CommBuffer and CommBufferSize parameters, allowing callers to corrupt either the firmware or the OS memory.

CVSS v3.1 Base Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2020-27339

CVE-2020-5953

A vulnerability exists in System Management Interrupt (SWSMI) handler of InsydeH2O UEFI firmware code located in SWSMI handler that dereferences gRT (EFI_RUNTIME_SERVICES) pointer to call a GetVariable service, which is located outside of SMRAM. This can result in code execution in SMM (escalating privilege from ring 0 to ring -2).

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/cve-2020-5953

CVE-2021-33625

An issue was discovered in Kernel 5.x in Insyde InsydeH2O, affecting HddPassword. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-33625

CVE-2021-33626

A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer(QWORD values for CommBuffer). This can be used by an attacker to corrupt data in SMRAM memory and even lead to arbitrary code execution

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-33626

CVE-2021-33627

An issue was discovered in Insyde InsydeH2O 5.x, affecting FwBlockServiceSmm. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses

CVSS v3.1 Base Score:	8.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-33627

CVE-2021-41837

An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score:	8.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-41837

CVE-2021-41838

An issue was discovered in SdHostDriver in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of a Numeric Range Comparison Without a Minimum Check.

CVSS v3.1 Base Score:	8.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-41838

CVE-2021-41839

An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score:	8.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-41839

CVE-2021-41841

An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.

CVSS v3.1 Base Score:	8.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-41841

CVE-2021-42059

An issue was discovered in Insyde InsydeH2O Kernel 5.0 before 05.08.41, Kernel 5.1 before 05.16.41, Kernel 5.2 before 05.26.41, Kernel 5.3 before 05.35.41, and Kernel 5.4 before 05.42.20. A stack-based buffer overflow leads toarbitrary code execution in UEFI DisplayTypeDxe DXE driver.

CVSS v3.1 Base Score:	6.7
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-42059

CVE-2021-42060

An issue was discovered in Insyde InsydeH2O Kernel 5.0 through 05.08.41, Kernel 5.1 through 05.16.41, Kernel 5.2 before 05.23.22, and Kernel 5.3 before 05.32.22. An Int15ServiceSmm SMM callout vulnerability

allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-42060

CVE-2021-42113

An issue was discovered in StorageSecurityCommandDxe in Insyde InsydeH2O with Kernel 5.1 before 05.14.28, Kernel 5.2 before 05.24.28, and Kernel 5.3 before 05.32.25. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-42113

CVE-2021-42554

An issue was discovered in Insyde InsydeH2O with Kernel 5.0 before 05.08.42, Kernel 5.1 before 05.16.42, Kernel 5.2 before 05.26.42, Kernel 5.3 before 05.35.42, Kernel 5.4 before 05.42.51, and Kernel 5.5 before 05.50.51. An SMM memory corruption vulnerability in FvbServicesRuntimeDxe allows a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-42554

CVE-2021-43323

An issue was discovered in UsbCoreDxe in Insyde InsydeH2O with kernel 5.5 before 05.51.45, 5.4 before 05.43.45, 5.3 before 05.35.45, 5.2 before 05.26.45, 5.1 before 05.16.45, and 5.0 before 05.08.45. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-43323

CVE-2021-43522

An issue was discovered in Insyde InsydeH2O with kernel 5.1 through 2021-11-08, 5.2 through 2021-11-08, and 5.3 through 2021-11-08. A StorageSecurityCommandDxe SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-43522

CVE-2021-43615

An issue was discovered in HddPassword in Insyde InsydeH2O with kernel 5.1 before 05.16.23, 5.2 before 05.26.23, 5.3 before 05.35.23, 5.4 before 05.43.22, and 5.5 before 05.51.22. An SMM memory corruption

vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-43615

CVE-2021-45969

An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the CommBuffer+8 location).

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-45969

CVE-2021-45970

An issue was discovered in IdeBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the status code saved at the CommBuffer+4 location).

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-45970

CVE-2021-45971

An issue was discovered in SdHostDriver in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (CommBufferData).

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-45971

CVE-2022-24030

An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-24030

CVE-2022-24031

An issue was discovered in NvmExpressDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2

CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-24031

CVE-2022-24069

An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.0 before 05.08.41, 5.1 before 05.16.29, 5.2 before 05.26.29, 5.3 before 05.35.29, 5.4 before 05.43.29, and 5.5 before 05.51.29. An SMM callout vulnerability allows an attacker to hijack the execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

CVSS v3.1 Base Score: 8.2
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-24069

Mitigating factors

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 vulnerabilities, they can help block known attack vectors.

An attacker needs elevated privileges to run code on affected systems to exploit the vulnerabilities listed above. B&R recommends restricting access and privileges to execute code to trusted entities on affected systems.

Frequently asked questions

What is the scope of these vulnerabilities?

An attacker who successfully exploits the most serious ones could run arbitrary code in an affected system node or potentially cause a denial of service condition.

What causes these vulnerabilities?

These vulnerabilities are caused by the issues in the InsydeH2O UEFI firmware in the B&R products listed above.

What is B&R APC?

APCs are Box PCs from B&R, designed and built to meet industrial customers' demands for maximum robustness, reliability, and long-term availability.

What is B&R PPC?

B&R Panel PCs (PPC) combine a display and a PC unit into a single extremely compact device and are available in a wide variety of display sizes with a touch or multi-touch screen and/or input keys.

What is B&R MPC?

B&R Automation PC mobile (MPC) with IP69K protection are industrial PCs, specially designed for use in harsh environments.

What might an attacker use these vulnerabilities to do?

An attacker who successfully exploits the most serious vulnerabilities could cause the affected system node to stop or become inaccessible or to insert and run arbitrary code with escalated privileges.

How could an attacker exploit these vulnerabilities?

An attacker needs access to affected products and privileges to run untrusted code to exploit the vulnerabilities.

Could these vulnerabilities be exploited remotely?

No, to exploit these vulnerabilities an attacker would need to have local access to an affected system node.

What does the update do?

The update removes all these vulnerabilities by applying the security patch for Insyde's InsydeH2O 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 these vulnerabilities were 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	
1.1	p3	Changed Release State of Updates	2023-03-24
1.2	p2, p3	Changed Release State of Updates	2023-04-17