

SSA-306654: Insyde BIOS Vulnerabilities in Siemens Industrial Products

Publication Date: 2022-02-22
Last Update: 2023-11-14
Current Version: V1.8
CVSS v3.1 Base Score: 8.4

SUMMARY

Insyde has published information on vulnerabilities in Insyde BIOS in [February 2022](#). This advisory lists the Siemens Industrial products affected by these vulnerabilities.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 ADM (6GK6015-0AL20-0GL0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 ADM CC (6GK6015-0AL20-0GL1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 CKP (6GK6015-0AL20-0GK0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 CKP CC (6GK6015-0AL20-0GK1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 CLOUDCONNECT (6GK6015-0AL20-0GM0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 CLOUDCONNECT CC (6GK6015-0AL20-0GM1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 ELAN (6GK6015-0AL20-0GP0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 ELAN CC (6GK6015-0AL20-0GP1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM APE1808 SAM-L (6GK6015-0AL20-0GN0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808 SAM-L CC (6GK6015-0AL20-0GN1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-P (6GK6015-0AL20-1AA0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-P CC (6GK6015-0AL20-1AA1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S1 (6GK6015-0AL20-1AB0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S1 CC (6GK6015-0AL20-1AB1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S3 (6GK6015-0AL20-1AD0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S3 CC (6GK6015-0AL20-1AD1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S5 (6GK6015-0AL20-1AF0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808CLA-S5 CC (6GK6015-0AL20-1AF1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808LNX (6GK6015-0AL20-0GH0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808LNX CC (6GK6015-0AL20-0GH1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM APE1808W10 (6GK6015-0AL20-0GJ0): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808W10 CC (6GK6015-0AL20-0GJ1): All Versions < V01.00.20_2N	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: All versions < V22.01.10	Update to V22.01.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: V22.01.10 affected by CVE-2021-43613	Update to V22.01.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All versions	Currently no fix is available https://support.industry.siemens.com/cs/ww/en/view/109763408/ See recommendations from section Workarounds and Mitigations
SIMATIC IPC127E: All versions < V27.01.09	Update BIOS to V27.01.09 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See recommendations from section Workarounds and Mitigations
SIMATIC IPC227G: All versions < V28.01.04	Update BIOS to V28.01.04 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC277G: All versions < V28.01.04	Update BIOS to V28.01.04 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC327G: All versions < V28.01.04	Update BIOS to V28.01.04 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations

SIMATIC IPC377G: All versions < V28.01.04	Update BIOS to V28.01.04 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC427E: All versions < V21.01.17	Update to V21.01.17 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC427E: All versions >= V21.01.17 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions < V21.01.17	Update to V21.01.17 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions >= V21.01.17 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions < V21.01.17	Update to V21.01.17 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions >= V21.01.17 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All versions < V25.02.12	Update to V25.02.12 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All versions >= V25.02.12 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All versions < V25.02.12	Update to V25.02.12 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations

SIMATIC IPC647E: All versions >= V25.02.12 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All versions < V25.02.12	Update to V25.02.12 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All versions >= V25.02.12 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions < V25.02.12	Update to V25.02.12 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions >= V25.02.12 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC ITP1000: All versions < V23.01.10	Update BIOS to V23.01.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITP1000: All versions >= V23.01.10 affected by CVE-2021-43613	Currently no fix is available See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- As a prerequisite for an attack, an attacker must be able to run untrusted code on affected systems. Siemens recommends limiting the possibilities to run untrusted code

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

PRODUCT DESCRIPTION

The RUGGEDCOM APE1808 is a powerful utility-grade application hosting platform that lets you deploy a range of commercially available applications for edge computing and cybersecurity in harsh, industrial environments.

SIMATIC Field PG is a mobile, industry-standard programming device for automation engineers with all commonly used interfaces for industrial applications that also brings pre-installed SIMATIC engineering software.

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based automation from Siemens.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (<https://www.first.org/cvss/>). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: <https://cwe.mitre.org/>.

Vulnerability 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 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
CWE	CWE-822: Untrusted Pointer Dereference

Vulnerability 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. The fixed versions for this issue in the AhciBusDxe, IdeBusDxe, NvmExpressDxe, SdHostDriverDxe, and SdMmcDeviceDxe drivers are 05.16.25, 05.26.25, 05.35.25, 05.43.25, and 05.51.25 (for Kernel 5.1 through 5.5).

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability 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 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
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-33626

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. The fixed versions for this issue in the PnpSmm, SmmResourceCheckDxe, and BeepStatusCode drivers are 05.08.23, 05.16.23, 05.26.23, 05.35.23, 05.43.23, and 05.51.23 (for Kernel 5.0 through 5.5).

CVSS v3.1 Base Score	7.8
CVSS 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
CWE	CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Vulnerability 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 Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-38489

An issue was discovered in the the HddPasswordPei driver of the Insyde InsydeH2O 5.x. HDD password is stored in plaintext.

CVSS v3.1 Base Score	7.8
CVSS 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
CWE	CWE-256: Plaintext Storage of a Password

Vulnerability 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 Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-41840

An issue was discovered in NvmExpressDxe 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Vulnerability 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 to arbitrary code execution in UEFI DisplayTypeDxe DXE driver.

CVSS v3.1 Base Score 6.7
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability 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 8.4
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability 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 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](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-43613

An issue was discovered in Insyde InsydeH2O 5.x, affecting SysPasswordDxe that exposes user and administrator password hashes in runtime UEFI variables, leading to escalation of privilege.

CVSS v3.1 Base Score 5.2
CVSS Vector [CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:O/RC:C](#)
CWE CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-43614

Error in handling the PlatformLangCodes UEFI variable in the VariableEditSmm driver could cause a buffer overflow, leading to resource exhaustion and failure.

CVSS v3.1 Base Score 6.7
CVSS Vector [CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C](#)
CWE CWE-400: Uncontrolled Resource Consumption

Vulnerability 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 Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability 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 8.4
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability 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 8.4
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability 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	8.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability 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	8.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability 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 Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability 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 Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

<https://www.siemens.com/cert/advisories>

HISTORY DATA

V1.0 (2022-02-22):	Publication Date
V1.1 (2022-03-08):	Corrected AV:L for all CVEs, added RUGGEDCOM APE1808 and SIMATIC IPC477E PRO
V1.2 (2022-07-12):	Added CVE-2021-43613, CVE-2021-43614 and CVE-2021-38489, add fix for SIMATIC Field PG M6, SIMATIC ITP1000 for all CVEs except CVE-2021-43613
V1.3 (2022-08-09):	Added fix for SIMATIC IPC227G, SIMATIC IPC277G, SIMATIC IPC327G, SIMATIC IPC377G, clarified affected versions for RUGGEDCOM APE1808
V1.4 (2022-10-11):	Added partial fix for SIMATIC IPC427E, SIMATIC IPC477E, SIMATIC IPC477E Pro
V1.5 (2023-02-14):	Added partial fix for SIMATIC IPC627E, SIMATIC IPC677E, SIMATIC IPC677E, and SIMATIC IPC847E
V1.6 (2023-07-11):	Added fix SIMATIC Field PG M5
V1.7 (2023-08-08):	Removed fix for SIMATIC Field PG M6 as fix version was withdrawn
V1.8 (2023-11-14):	Added fix for SIMATIC IPC127E

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.