# SSA-306654: Insyde BIOS Vulnerabilities in Siemens Industrial Products

Publication Date: 2022-02-22
Last Update: 2025-04-08
Current Version: V1.9
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 has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| RUGGEDCOM APE1808 - BIOS:<br>All versions < V1.0.202N<br>affected by CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, 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-2021-43613, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V1.0.202N or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109814796/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC Field PG: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC Field PG M5: | See below<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC Field PG M5:<br>All versions < V22.01.10<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V22.01.10 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC Field PG M5:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC Field PG M6:<br>All versions < V26.01.13<br>affected by all CVEs | Update to V26.01.13 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC family: | Update to V27.01.09 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC127E:<br>All versions < V27.01.09<br>affected by all CVEs | Update to V27.01.09 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC227G / IPC277G / IPC277G PRO / IPC327G / IPC377G: | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC227G:<br>All versions < V28.01.04<br>affected by all CVEs | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC277G:<br>All versions < V28.01.04<br>affected by all CVEs | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC277G PRO:<br>All versions < V28.01.04<br>affected by all CVEs | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC327G:<br>All versions < V28.01.04<br>affected by all CVEs | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC IPC377G:<br>All versions < V28.01.04<br>affected by all CVEs | Update to V28.01.04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC427E / IPC477E / IPC477E PRO: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC427E: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC427E:<br>All versions < V21.01.17<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V21.01.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC427E:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC IPC477E: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC477E:<br>All versions < V21.01.17<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V21.01.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC477E:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC IPC477E PRO: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC477E PRO:<br>All versions < V21.01.17<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V21.01.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC477E PRO:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS IPC427E: | See below<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS IPC427E:<br>All versions < V21.01.17<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V21.01.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS IPC427E:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC IPC627E / IPC647E / IPC677E / IPC847E: | See below<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC IPC627E: | See below<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC627E:<br>All versions < V25.02.12<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V25.02.12 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC627E:<br>All versions < V25.02.15<br>affected by CVE-2021-43613 | Update to V25.02.15 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC647E: | See below<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC647E:<br>All versions < V25.02.12<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V25.02.12 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC647E:<br>All versions < V25.02.15<br>affected by CVE-2021-43613 | Update to V25.02.15 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC IPC677E: | See below<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC677E:<br>All versions < V25.02.12<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V25.02.12 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC677E:<br>All versions < V25.02.15<br>affected by CVE-2021-43613 | Update to V25.02.15 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC847E: | See below<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC847E:<br>All versions < V25.02.12<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V25.02.12 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC IPC847E:<br>All versions < V25.02.15<br>affected by CVE-2021-43613 | Update to V25.02.15 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ITP1000: | See below<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ITP1000:<br>All versions < V23.01.10<br>affected by CVE-2020-5953, CVE-2020-27339, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-38489, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41840, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43614, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069 | Update to V23.01.10 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763408/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ITP1000:<br>All versions<br>affected by CVE-2021-43613 | Currently no fix is available<br>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

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 toarbitrary 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| CWE | CWE-20: Improper Input Validation |

## ADDITIONAL INFORMATION

For RUGGEDCOM APE1808 devices use the APE software upgrade tool (https://support.industry.siemens.com/cs/ww/en/view/109814796/) to update the BIOS version.

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 |
| V1.9 (2025-04-08): | Added fix for all CVE IDs for SIMATIC Field PG M6; Added fix for CVE-2021-43613 for SIMATIC IPC627E / IPC647E / IPC677E / IPC847E; Removed fix for CVE-2021-43613 for SIMATIC Field PG M5 as this CVE was not fixed in version V22.01.11; RUGGEDCOM APE1808 - BIOS: Removed CVE-2020-5953, CVE-2021-41840 and CVE-2021-43614 as not affected; added the link to the APE software upgrade tool to apply a BIOS version that fixes the other CVE IDs |

## TERMS OF USE