SSA-450613: Insyde BIOS Vulnerabilities in RUGGEDCOM APE1808 Product Family

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.0

SUMMARY

Insyde has published information on vulnerabilities in Insyde BIOS in November 2022. These vulnerabilities also affect the RUGGEDCOM APE1808 product family.

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	Currently no fix is available
RUGGEDCOM APE1808 ADM CC (6GK6015-0AL20-0GL1): All versions	Currently no fix is available
RUGGEDCOM APE1808 CKP (6GK6015-0AL20-0GK0): All versions	Currently no fix is available
RUGGEDCOM APE1808 CKP CC (6GK6015-0AL20-0GK1): All versions	Currently no fix is available
RUGGEDCOM APE1808 CLOUDCONNECT (6GK6015-0AL20-0GM0): All versions	Currently no fix is available
RUGGEDCOM APE1808 CLOUDCONNECT CC (6GK6015-0AL20-0GM1): All versions	Currently no fix is available
RUGGEDCOM APE1808 ELAN (6GK6015-0AL20-0GP0): All versions	Currently no fix is available
RUGGEDCOM APE1808 ELAN CC (6GK6015-0AL20-0GP1): All versions	Currently no fix is available
RUGGEDCOM APE1808 SAM-L (6GK6015-0AL20-0GN0): All versions	Currently no fix is available

RUGGEDCOM APE1808 SAM-L CC (6GK6015-0AL20-0GN1): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-P (6GK6015-0AL20-1AA0): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-P CC (6GK6015-0AL20-1AA1): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S1 (6GK6015-0AL20-1AB0): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S1 CC (6GK6015-0AL20-1AB1): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S3 (6GK6015-0AL20-1AD0): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S3 CC (6GK6015-0AL20-1AD1): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S5 (6GK6015-0AL20-1AF0): All versions	Currently no fix is available
RUGGEDCOM APE1808CLA-S5 CC (6GK6015-0AL20-1AF1): All versions	Currently no fix is available
RUGGEDCOM APE1808LNX (6GK6015-0AL20-0GH0): All versions	Currently no fix is available
RUGGEDCOM APE1808LNX CC (6GK6015-0AL20-0GH1): All versions	Currently no fix is available
RUGGEDCOM APE1808W10 (6GK6015-0AL20-0GJ0): All versions	Currently no fix is available
RUGGEDCOM APE1808W10 CC (6GK6015-0AL20-0GJ1): All versions	Currently no fix is available

WORKAROUNDS AND MITIGATIONS

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.

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-2022-30774

DMA attacks on the parameter buffer used by the PnpSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack). This issue was discovered by Insyde engineering during a security review. https://www.insyde.com/security-pledge/SA-2022043

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-31243

Update description and links DMA transactions which are targeted at input buffers used for the software SMI handler used by the FvbServicesRuntimeDxe driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. https://www.insyde.com/security-pledge/SA-2022044

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-33906

DMA transactions which are targeted at input buffers used for the FwBlockServiceSmm software SMI handler could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. https://www.insyde.com/security-pledge/SA-2022048

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-33907

DMA transactions which are targeted at input buffers used for the software SMI handler used by the IdeBusDxe driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. https://www.insyde.com/security-pledge/SA-2022049

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-33908

DMA transactions which are targeted at input buffers used for the SdHostDriver software SMI handler could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. https://www.insyde.com/security-pledge/SA-2022050

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-33982

DMA attacks on the parameter buffer used by the Int15ServiceSmm software SMI handler could lead to a TOCTOU attack on the SMI handler and lead to corruption of SMRAM. This issue was discovered by Insyde engineering during a security review.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Vulnerability CVE-2022-33984

DMA transactions which are targeted at input buffers used for the SdMmcDevice software SMI handler could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. https://www.insyde.com/security-pledge/SA-2022054

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

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 (2023-02-14): Publication Date

TERMS OF USE