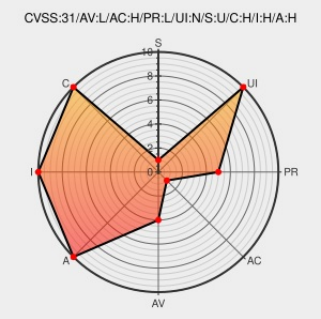
CVE-2022-32477

Published on: Not Yet Published

Last Modified on: 02/25/2023 03:27:00 AM UTC

CVE-2022-32477

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Insydeh2o from Insyde contain the following vulnerability:

An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the FvbServicesRuntimeDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it.

CVE-2022-32477 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Insyde's Security Pledge | Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge
Insyde Security Advisory 2023009 | Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge/SA-2023009

There are currently no QIDs associated with this CVE

Exploit/POC from Github

An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the FvbServicesRuntimeDxe sha…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Insyde	Insydeh2o	All	All	All	All

cpe:2.3:a:insyde:insydeh2o:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32477 : An issue was discovered in Insyde InsydeH2O with #kernel 5.0 through 5.5. DMA attacks on the FvbSe… twitter.com/i/web/status/1…	2023-02-15 14:07:19
@JohnJasonFallow	New vulnerability on the NVD: CVE-2022-32477 ift.tt/q2tQ3BF	2023-02-15 15:11:40
@doogsineerg	New vulnerability on the NVD: CVE-2022-32477 ift.tt/8riILfb	2023-02-15 15:33:29
/r/netcve	CVE-2022-32477	2023-02-15 15:38:44

← Previous ID

Next ID→