



CVE-2022-32477

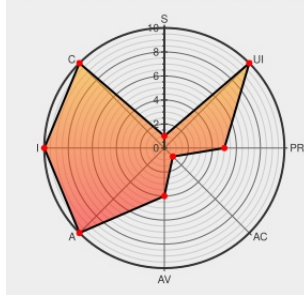
Published on: Not Yet Published

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

CVE-2022-32477

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H



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 [M](#) 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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/8rilLfb	2023-02-15 15:33:29
 /r/netcve	CVE-2022-32477	2023-02-15 15:38:44

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)