



CVE-2022-35408

Published on: Not Yet Published

Last Modified on: 09/23/2022 07:03:00 PM UTC

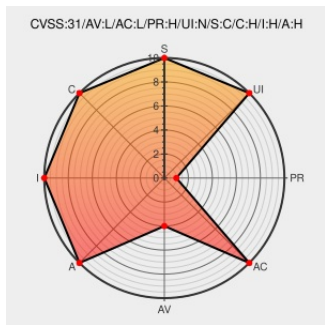
CVE-2022-35408

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. An SMM callout vulnerability in the SMM driver in `UsbLegacyControlSmm` leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the `EFI_BOOT_SERVICES` table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.)

CVE-2022-35408 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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
[BRLY-2022-022] SMM callout vulnerability in SMM driver (SMM arbitrary code execution).	binary.io text/html	MISC binary.io/advisories/BRLY-2022-022/index.html
Insyde Security Advisory 2022031 Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge/SA-2022031

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

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-2022-35408 : An issue was discovered in Insyde InsydeH2O with #kernel 5.0 through 5.5. An SMM callout vulnerabi... twitter.com/i/web/status/1...	2022-09-22 16:05:03
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-35408 An issue was discovered in Insyde InsydeH2O with kernel 5.0 throu... twitter.com/i/web/status/1...	2022-09-22 16:55:59
 /r/netcve	CVE-2022-35408	2022-09-22 16:38:46

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)