



CVE-2022-33986

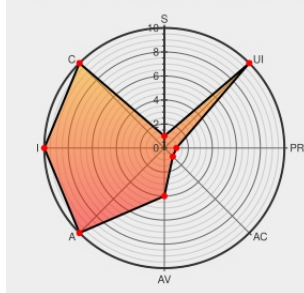
Published on: Not Yet Published

Last Modified on: 11/18/2022 03:48:00 PM UTC

CVE-2022-33986

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

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



Certain versions of [Kernel](#) from [Insyde](#) contain the following vulnerability:

DMA attacks on the parameter buffer used by the VariableRuntimeDxe software SMI handler could lead to a TOCTOU attack. DMA attacks on the parameter buffer used by the software SMI handler used by the driver VariableRuntimeDxe 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. This issue is fixed in Kernel 5.4: 05.44.23 and Kernel 5.5: 05.52.23. CWE-367 CWE-367 Report at: <https://www.insyde.com/security-pledge/SA-2022056>

CVE-2022-33986 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	HIGH	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 2022056 Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge/SA-2022056

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	Kernel	All	All	All	All
cpe:2.3:a:insyde:kernel:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-33986 : DMA attacks on the parameter buffer used by the VariableRuntimeDxe software SMI handler could lead... twitter.com/i/web/status/1...	2022-11-15 00:10:16
 /r/LenovoLegion	Legion 5 Pro 16IAH7H - BIOS Update (J2CN46WW)	2022-11-08 14:55:10
 /r/netcve	CVE-2022-33986	2022-11-15 01:38:51

[← 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](#)