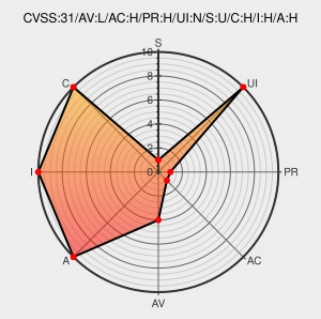
CVE-2022-31243

Published on: Not Yet Published

Last Modified on: 02/14/2023 12:15:00 PM UTC

CVE-2022-31243

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



Certain versions of Kernel from Insyde contain the following vulnerability:

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.. "DMA transactions which are targeted at input buffers used for the software SMI handler used by the FvbServicesRuntimeDxe driver could cause SMRAM corruption. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in Kernel 5.2: 05.27.21. Kernel 5.3: 05.36.21. Kernel 5.4: 05.44.21. Kernel 5.5: 05.52.21 https://www.insyde.com/security-pledge/SA-2022044

CVE-2022-31243 has been assigned by 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 Security Advisory 2022044 | Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge/SA-2022044
Insyde's Security Pledge | Insyde Software	www.insyde.com text/html	MISC www.insyde.com/security-pledge
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-450613.pdf

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-2022-31243 : Update description and links DMA transactions which are targeted at input buffers used for the sof… twitter.com/i/web/status/1…	2022-11-15 00:07:08
/r/LenovoLegion	Legion 5 Pro 16IAH7H - BIOS Update (J2CN46WW)	2022-11-08 14:55:10
/r/netcve	CVE-2022-31243	2022-11-15 01:38:45

← Previous ID

Next ID→