



# CVE-2022-31243

Published on: Not Yet Published

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

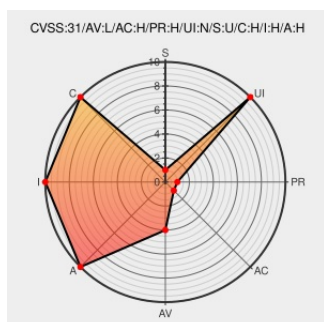
## CVE-2022-31243

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 [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    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>HIGH</b>            | <b>HIGH</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

## CVE References

| Description                                        | Tags                                                                                                                     | Link                                                                                                                                        |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Insyde Security Advisory 2022044   Insyde Software | <a href="https://www.insyde.com/text/html">www.insyde.com</a><br><a href="#">text/html</a>                               | <a href="https://www.insyde.com/security-pledge/SA-2022044">MISC www.insyde.com/security-pledge/SA-2022044</a>                              |
| Insyde's Security Pledge   Insyde Software         | <a href="https://www.insyde.com/text/html">www.insyde.com</a><br><a href="#">text/html</a>                               | <a href="https://www.insyde.com/security-pledge">MISC www.insyde.com/security-pledge</a>                                                    |
|                                                    | <a href="https://cert-portal.siemens.com/application/pdf">cert-portal.siemens.com</a><br><a href="#">application/pdf</a> | <a href="https://cert-portal.siemens.com/productcert/pdf/ssa-450613.pdf">CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-450613.pdf</a> |

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](mailto: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                               | <a href="#">Insyde</a> | <a href="#">Kernel</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-11-15<br>00:07:08 |
|  <a href="#">/r/LenovoLegion</a> | <a href="#">Legion 5 Pro 16IAH7H - BIOS Update (J2CN46WW)</a>                                                                                                                                            | 2022-11-08<br>14:55:10 |
|  <a href="#">/r/netcve</a>       | <a href="#">CVE-2022-31243</a>                                                                                                                                                                           | 2022-11-15<br>01:38:45 |

[← 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](#)