



# CVE-2021-4210

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-4210
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@lenovo.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-22 21:15:00 UTC
<b>Updated</b>	2022-08-09 00:21:00 UTC
<b>Description</b>	A potential vulnerability in the SMI callback function used in the NVME driver in some Lenovo Desktop, ThinkStation, and T

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Lenovo	A540-24icb	-	All	All	All
Operating System	Lenovo	A540-24icb Firmware	-	All	All	All
Hardware	Lenovo	A540-27icb	-	All	All	All
Operating System	Lenovo	A540-27icb Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre 5-14imb05	-	All	All	All
Operating System	Lenovo	Ideacentre 5-14imb05 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-22ada6	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-22ada6 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-22iil5	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-22iil5 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-22itl6	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-22itl6 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-24ada6	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-24ada6 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-24iil5	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-24iil5 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-24itl6	-	All	All	All

Operating System	Lenovo	Ideacentre Aio 3-24itl6 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre Aio 3-27itl6	-	All	All	All
Operating System	Lenovo	Ideacentre Aio 3-27itl6 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre C5-14imb05	-	All	All	All
Operating System	Lenovo	Ideacentre C5-14imb05 Firmware	-	All	All	All
Hardware	Lenovo	Ideacentre G5-14imb05	-	All	All	All
Operating System	Lenovo	Ideacentre G5-14imb05 Firmware	-	All	All	All
Hardware	Lenovo	Stadia Ggp-120	-	All	All	All
Operating System	Lenovo	Stadia Ggp-120 Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M700	-	All	All	All
Operating System	Lenovo	Thinkcentre M700 Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M700 Tiny	-	All	All	All
Operating System	Lenovo	Thinkcentre M700 Tiny Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M70a	-	All	All	All
Operating System	Lenovo	Thinkcentre M70a Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M75n	-	All	All	All
Operating System	Lenovo	Thinkcentre M75n Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M800	-	All	All	All
Operating System	Lenovo	Thinkcentre M800 Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M810z	-	All	All	All
Operating System	Lenovo	Thinkcentre M810z Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M820z	-	All	All	All
Operating System	Lenovo	Thinkcentre M820z Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M900	-	All	All	All
Hardware	Lenovo	Thinkcentre M900x	-	All	All	All
Operating System	Lenovo	Thinkcentre M900x Firmware	-	All	All	All
Operating System	Lenovo	Thinkcentre M900 Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M90a Gen2	-	All	All	All
Operating System	Lenovo	Thinkcentre M90a Gen2 Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre M910z	-	All	All	All
Operating System	Lenovo	Thinkcentre M910z Firmware	-	All	All	All
Hardware	Lenovo	Thinkcentre X1	-	All	All	All
Operating System	Lenovo	Thinkcentre X1 Firmware	-	All	All	All
Hardware	Lenovo	Thinkedge Se30	-	All	All	All
Operating System	Lenovo	Thinkedge Se30 Firmware	-	All	All	All

Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkstation P310</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinkstation P310 Firmware</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkstation P520</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkstation P520c</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinkstation P520c Firmware</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinkstation P520 Firmware</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">V410z</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">V410z Firmware</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">V50t-13imb</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">V50t-13imb Firmware</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">V540-24iwl</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">V540-24iwl Firmware</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Multi-vendor BIOS Security Vulnerabilities (February 2022) - Lenovo Support US	MISC	<a href="https://support.lenovo.com">support.lenovo.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Lenovo thanks Jiawei Yin(@yngweijw) and Menghao Li of IIE varas

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](https://status.cve.report)