



# CVE-2021-3452

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-3452
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@lenovo.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-16 21:15:00 UTC
<b>Updated</b>	2021-07-27 16:48:00 UTC
<b>Description</b>	A potential vulnerability in the system shutdown SMI callback function in some ThinkPad models may allow an attacker with

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Lenovo</a>	<a href="#">Bios</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Bios</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad 11e 3rd Gen</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad 11e 4th Gen</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad 11e 5th Gen</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad 11e Yoga Gen 6</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad 13 Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad E14 Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad E15 Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L13</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L13 Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L13 Yoga</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L13 Yogo Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L14</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L14 Gen 2</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L15</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L15 Gen 2</a>	-	All	All	All

Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L380</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L380 Yoga</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L390</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad L390 Yoga</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad T460</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad X12 Detachable Gen 1</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad X260</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad X380 Yoga</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad Yoga 11e 3rd Gen</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad Yoga 11e 4th Gen</a>	-	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkpad Yoga 370</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Lenovo BIOS Vulnerabilities (July 2021) - 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 Binarly efiXplorer team for reporting these issues.

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)