



# CVE-2021-3849

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

## Summary

<b>CVE</b>	CVE-2021-3849
<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>	2022-10-27 11:55:00 UTC
<b>Description</b>	An authentication bypass vulnerability was discovered in the web interface of the Lenovo Fan Power Controller2 (FPC2) an

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">ibm</a>	<a href="#">Nextscale Fan Power Controller</a>	-	All	All	All
Operating System	<a href="#">ibm</a>	<a href="#">Nextscale Fan Power Controller Firmware</a>	All	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Nextscale N1200 Enclosure</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Nextscale N1200 Enclosure Firmware</a>	All	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkagile Hx Enclosure Certified Node</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinkagile Hx Enclosure Certified Node Firmware</a>	All	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinkagile Vx Enclosure</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinkagile Vx Enclosure Firmware</a>	All	All	All	All
Hardware	<a href="#">Lenovo</a>	<a href="#">Thinksystem D2 Enclosure</a>	-	All	All	All
Operating System	<a href="#">Lenovo</a>	<a href="#">Thinksystem D2 Enclosure Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Authentication Bypass Vulnerabilities in FPC2 and SMM Firmware - Lenovo Support US	CONFIRM	<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, anal

No vendor comments have been submitted for this CVE.

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](#)**