



CVE-2022-0354

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

Summary

CVE	CVE-2022-0354
State	PUBLIC
Assigner	psirt@lenovo.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-22 21:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	A vulnerability was reported in Lenovo System Update that could allow a local user with interactive system access the ability to escalate their privileges and gain root access to the system.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lenovo	System Update	All	All	All	All

References

Reference	Source	Link	Tags
Lenovo System Update Privilege Escalation Vulnerability - Lenovo Support US	MISC	support.lenovo.com	
CVE-2022-0354: Local Privilege Escalation - infosec.tirol	MISC	www.infosec.tirol	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Lenovo thanks Daniel Feichter (@VirtualAllocEx) at Infosec Tirol for reporting this issue.

Legacy QID Mappings

[376718](#) Lenovo System Update Privilege Escalation Vulnerability (len-76673)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)