



# CVE-2026-1636

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

## Summary

<b>CVE</b>	CVE-2026-1636
<b>State</b>	PUBLISHED
<b>Assigner</b>	lenovo
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 13:16:24 UTC
<b>Updated</b>	2026-04-17 15:09:46 UTC
<b>Description</b>	A potential DLL hijacking vulnerability was reported in Lenovo Service Bridge that, under certain conditions, could allow a local user to execute arbitrary code with system privileges.

## Risk And Classification

**Primary CVSS:** v4.0 5.4 MEDIUM from psirt@lenovo.com

**CVSS:** 4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000140000 probability, percentile 0.023500000 (date 2026-04-17)

**Problem Types:** CWE-427 | CWE-427 CWE-427: Uncontrolled Search Path Element

Version	Source	Type	Score	Severity	Vector
4.0	psirt@lenovo.com	Secondary	5.4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	5.4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	psirt@lenovo.com	Primary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Lenovo	Service Bridge	affected 5.0.2.20 custom	Not specified

### References

Reference	Source	Link	Tags
support.lenovo.com/us/en/product-security/EN-014074	psirt@lenovo.com	support.lenovo.com	

<a href="https://support.lenovo.com/us/en/product_security/LEIN-211071">support.lenovo.com/us/en/product_security/LEIN-211071</a>	<a href="mailto:psirt@lenovo.com">psirt@lenovo.com</a>	<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

**CNA:** Lenovo thanks Victor Rodriguez (aka NT3P) for reporting this issue. (en)

### Additional Advisory Data

#### Solutions

**CNA:** Upgrade to the Lenovo Service Bridge version 5.0.2.20 or later. Lenovo Service Bridge is updated automatically.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)