CVE-2026-1636

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-1636
State	PUBLISHED
Assigner	lenovo
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 13:16:24 UTC
Updated	2026-04-17 15:09:46 UTC
Description	A potential DLL hijacking vulnerability was reported in Lenovo Service Bridge that, under certain conditions, could allow a lo

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/MSC:X/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/C..
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

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/MSC:X/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/LEN-211071	psirt@lenovo.com	support.lenovo.com	

support.lenovo.com/us/en/product_security/LEN-21107	psirt@lenovo.com	support.lenovo.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.