CVE-2026-6282

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

Summary

CVE	CVE-2026-6282
State	PUBLISHED
Assigner	lenovo
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 16:17:01 UTC
Updated	2026-05-13 16:27:11 UTC
Description	A potential improper file path validation vulnerability was reported in some Lenovo Personal Cloud Storage devices that cou

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from psirt@lenovo.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/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

Problem Types: CWE-22 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	psirt@lenovo.com	Secondary	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C..
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
3.1	psirt@lenovo.com	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/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

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Lenovo	Personal Cloud T2s	affected 5.5.6.t2s.3 custom	Not specified
CNA	Lenovo	Personal Cloud T2Pro	affected 5.4.8.t2pro.2 custom	Not specified
CNA	Lenovo	Personal Cloud X1s	affected 5.4.8.x1s.2 custom	Not specified
CNA	Lenovo	Home Storage Hub T20	affected 5.5.8.t20.1 custom	Not specified
CNA	Lenovo	Home Storage Hub X20	affected 5.4.4.x20.1 custom	Not specified

CNA	Lenovo	Home Storage Hub X20	affected 5.4.4.x20.1 custom	Not specified
CNA	Lenovo	Personal Cloud T1	affected 5.4.0.t1.6 custom	Not specified
CNA	Lenovo	Personal Cloud A1	affected 5.4.2.a1.3 custom	Not specified
CNA	Lenovo	Personal Cloud A1s	affected 5.5.6.a1s custom	Not specified
CNA	Lenovo	Personal Cloud T2	affected 5.4.5.t2.2 custom	Not specified
CNA	Lenovo	Personal Cloud X1	affected 5.4.7.x1.1 custom	Not specified

References

Reference	Source	Link	Tags
pc.lenovo.com.cn/tips/Ann/t1_eol.html	psirt@lenovo.com	pc.lenovo.com.cn	
iknow.lenovo.com.cn/detail/440274	psirt@lenovo.com	iknow.lenovo.com.cn	
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 Wang Jincheng, Professor Yu Le from Nanjing University of Posts and Telecommunications and Professor Luo Xiapu from The Hong Kong Polytechnic University (en)

Additional Advisory Data

Solutions

CNA: Update device firmware to the version indicated in the advisory: https://iknow.lenovo.com.cn/detail/440274

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