pyLoad has an incomplete fix for CVE-2026-33509: unprotected storage_folder enables arbitrary file write to Flask session store and code execution

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

Summary

CVE	CVE-2026-35464
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 15:17:44 UTC
Updated	2026-04-07 17:16:30 UTC
Description	pyLoad is a free and open-source download manager written in Python. The fix for CVE-2026-33509 added an ADMIN_ON

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

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

Problem Types: CWE-502 | CWE-863 | CWE-502 CWE-502: Deserialization of Untrusted Data | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pyload	Pyload	affected <= 0.5.0b3.dev96	Not specified

References

Reference	Source	Link
github.com/pyload/pyload/security/advisories/GHSA-4744-96p5-mp2j	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/pyload/pyload/commit/c4cf995a2803bdbe388addfc2b0f323277efc0e1	security-advisories@github.com	github.com
www.cve.org/CVERecord	security-advisories@github.com	www.cve.org
github.com/pyload/pyload/security/advisories/GHSA-r7mc-x6x7-cqxx	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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