pypdf: Manipulated FlateDecode predictor parameters can exhaust RAM

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

Summary

CVE	CVE-2026-41312
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 22:16:32 UTC
Updated	2026-04-22 22:16:32 UTC
Description	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions prior to 6

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/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-789 | CWE-789 CWE-789: Memory Allocation with Excessive Size Value

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/S
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

ntegrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Py-pdf	Pypdf	affected < 6.10.2	Not specified

References

Reference	Source	Link	Tags
github.com/py-pdf/pypdf/releases/tag/6.10.2	security-advisories@github.com	github.com	
github.com/py-pdf/pypdf/commit/ac734dab4eef92bcce50d503949b4d9887d89f11	security-advisories@github.com	github.com	
github.com/py-pdf/pypdf/security/advisories/GHSA-7gw9-cf7v-778f	security-advisories@github.com	github.com	
github.com/py-pdf/pypdf/pull/3734	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report