



CVE-2023-36464

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-36464
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-27 22:15:00 UTC
Updated	2023-07-06 16:13:00 UTC
Description	pypdf is an open source, pure-python PDF library. In affected versions an attacker may craft a PDF which leads to an infinit

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pypdf2 Project	Pypdf2	All	All	All	All
Application	Pypdf Project	Pypdf	All	All	All	All

References

Reference	Source
Possible Infinite Loop when a comment isn't followed by a character · Advisory · py-pdf/pypdf · GitHub	MISC
BUG: Prevent infinite loop when no character follows after a comment by exiledkingcc · Pull Request #1828 · py-pdf/pypdf · GitHub	MISC
improved ExtractText(3) by pubpub-zz · Pull Request #969 · py-pdf/pypdf · GitHub	MISC
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)