



# CVE-2023-46250

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-46250
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-31 16:15:00 UTC
<b>Updated</b>	2023-11-08 17:51:00 UTC
<b>Description</b>	pypdf is a free and open-source pure-python PDF library. An attacker who uses a vulnerability present in versions 3.7.0 thro

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Pypdf Project</a>	<a href="#">Pypdf</a>	All	All	All	All

## References

Reference	Source
SEC: Infinite recursion when using PdfWriter(clone_from=reader) (#2264) · py-pdf/pypdf@9b23ac3 · GitHub	MISC
Possible Infinite Loop when PdfWriter(clone_from) is used with a PDF · Advisory · py-pdf/pypdf · GitHub	MISC
BUG: Infinite recursion when using PdfWriter(clone_from=reader) by Alexhuszagh · Pull Request #2264 · py-pdf/pypdf · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[995796](#) Python (Pip) Security Update for pypdf (GHSA-wjcc-cq79-p63f)

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](#)