

py-pdf / **pypdf** Public[Code](#) [Issues](#) 95 [Pull requests](#) 28 [Discussions](#) [Actions](#) [Security and](#)

# Manipulated XMP metadata entity declarations can exhaust RAM

Moderate stefan6419846 published GHSA-3crg-w4f6-42mx last week

## Package

 **pypdf** (pip)

### Affected versions

&lt; 6.10.0

### Patched versions

&gt;= 6.10.0

## Description

### Impact

An attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires parsing the XMP metadata.

### Patches

This has been fixed in [pypdf==6.10.0](#).

### Workarounds

If you cannot upgrade yet, consider applying the changes from PR [#3724](#).

## Severity

Moderate

## CVE ID

CVE-2026-40260

## Weaknesses

▶ CWE-776

---

### Credits



**kodareef5**

Reporter



**stefan6419846**

Analyst