py-pdf / **PyPDF2** Public

Code | Issues 70 | Pull requests 11 | Discussions | Actions | **Security** 1 ...

Manipulated inline images can cause Infinite Loop

Moderate **MartinThoma** published **GHSA-xcjx-m2pj-8g79** on Apr 17

Package

PyPDF2 (pip)

Affected versions	Patched versions
<=1.27.4	1.27.5

Description

Impact

An attacker who uses this vulnerability can craft a PDF which leads to an infinite loop if the PyPDF2 user wrote the following code:

```
from PyPDF2 import PdfFileReader, PdfFileWriter
from PyPDF2.pdf import ContentStream

reader = PdfFileReader("malicious.pdf", strict=False)
for page in reader.pages:
    ContentStream(page.getContents(), reader)
```

Patches

`PyPDF2==1.27.5` and later are patched.

Credits to Sebastian Krause for finding (issue) and fixing (PR) it.

Severity

Moderate 6.2 / 10

CVSS base metrics

Attack vector	**Local**
Attack complexity	**Low**
Privileges required	**None**
User interaction	**None**
Scope	**Unchanged**
Confidentiality	**None**
Integrity	**None**
Availability	**High**

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

CVE ID

CVE-2022-24859

Weaknesses

No CWEs