

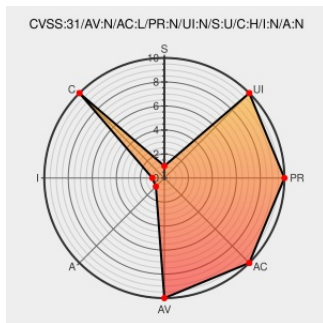


# CVE-2021-29421

Published on: 04/01/2021 12:00:00 AM UTC

Last Modified on: 12/03/2022 02:25:00 PM UTC

## CVE-2021-29421

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

models/metadata.py in the pikepdf package 1.3.0 through 2.9.2 for Python allows XXE when parsing XMP metadata entries.

CVE-2021-29421 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description                                                     | Tags                                                    | Link                                                                                      |
|-----------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------------------------|
| pikepdf/release_notes.rst at v2.10.0 · pikepdf/pikepdf · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/pikepdf/pikepdf/blob/v2.10.0/docs/release_notes.rst#v2100</a> |
| [SECURITY] Fedora 33                                            | <a href="#">lists.fedoraproject.org</a>                 | <a href="#">FEDORA FEDORA-2021-4bf9909a76</a>                                             |

Update: python-pikepdf-  
1.19.4-2.fc33 - package-  
announce - Fedora Mailing-  
Lists

[text/html](#)

Fix XXE vulnerability in XMP  
metadata parsing ·  
pikepdf/pikepdf@3f38f73 ·  
GitHub

[github.com](#)

[text/html](#)



CONFIRM

[github.com/pikepdf/pikepdf/commit/3f38f73218e5e782fe411ccbb3b44a793c0b343a](https://github.com/pikepdf/pikepdf/commit/3f38f73218e5e782fe411ccbb3b44a793c0b343a)

[SECURITY] Fedora 32  
Update: python-pikepdf-  
1.19.4-2.fc32 - package-  
announce - Fedora Mailing-  
Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org)

[text/html](#)



FEDORA FEDORA-2021-d97bc581be

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

[179883](#) Debian Security Update for pikepdf (CVE-2021-29421)

[281382](#) Fedora Security Update for python (FEDORA-2021-d97bc581be)

[281383](#) Fedora Security Update for python (FEDORA-2021-4bf9909a76)

[501904](#) Alpine Linux Security Update for py3-pikepdf

[980634](#) Python (pip) Security Update for pikepdf (GHSA-ccgm-3xw4-h5p8)

## Exploit/POC from Github

models/metadata.py in the pikepdf package 1.3.0 through 2.9.2 for Python allows XXE when parsing XMP metadata entries...

## Known Affected Configurations (CPE V2.3)

| Type                                                         | Vendor                          | Product                 | Version | Update | Edition | Language |
|--------------------------------------------------------------|---------------------------------|-------------------------|---------|--------|---------|----------|
| Operating System                                             | <a href="#">Fedoraproject</a>   | <a href="#">Fedora</a>  | 32      | All    | All     | All      |
| Operating System                                             | <a href="#">Fedoraproject</a>   | <a href="#">Fedora</a>  | 33      | All    | All     | All      |
| Application                                                  | <a href="#">Pikepdf Project</a> | <a href="#">Pikepdf</a> | All     | All    | All     | All      |
| <a href="#">cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:</a> |                                 |                         |         |        |         |          |
| <a href="#">cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:</a> |                                 |                         |         |        |         |          |
| <a href="#">cpe:2.3:a:pikepdf_project:pikepdf:*:*:*:*:*:</a> |                                 |                         |         |        |         |          |

No vendor comments have been submitted for this CVE

| Social Mentions                                                                             |                                                                                                                                                                                                          |                           |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Source                                                                                      | Title                                                                                                                                                                                                    | Posted (UTC)              |
|  @CVEreport | CVE-2021-29421 : models/metadata.py in the pikepdf package 1.3.0 through 2.9.2 for Python allows XXE when parsing X... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-04-01<br>20:05:09    |
| <a href="#">← Previous ID</a>                                                               |                                                                                                                                                                                                          | <a href="#">Next ID →</a> |

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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