Dockerfile
README.md
exampleInput.txt
exampleOutput.csv
exampleOutput.json
exampleOutput.txt
requirements.txt
sshUsernameEnumEx...

README

CVE-2018-15473-Exploit

On August 15th, 2018, the following advisory was posted on the OSS-Security list: http://openwall.com/lists/oss-security/2018/08/15/5

About

Exploit written in Python for CVE-2018-15473 with threading and export formats

Readme
Activity
519 stars
21 watching
183 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 5

Languages

Python 93.7% Dockerfile 6.3%

The ShellIntel team decided to invest some time and write an exploit for this vulnerability. The exploit below has the following features:

- Threading - default 5
  - If more than 10 are used, often the OpenSSH service gets overwhelmed and causes retries
- Single username evaluation via `username` parameter
- Multiple username evaluation via `userList` parameter
- Multiple username evaluation file output via `outputFile` parameter
- Multiple output formats (list, json, csv) via `outputFormat` parameter

An example username input file is given in `exampleInput.txt`
An example results output file in List format is given in `exampleOutput.txt`
An example results output file in JSON format is given in `exampleOutput.json`
An example results output file in CSV format is given in `exampleOutput.csv`

Install the dependencies by running `pip install -r requirements.txt`

=======

Build the image:

docker build -t cve-2018-15473 .

Run the exploit:

docker run cve-2018-15473 -h

Delete containers and image:

```
docker ps -a | awk '$2 == "cve-2018-15473" {print $1}' | xargs
```