New issue

Jump to bottom

[security] Path traversal due to incorrect input sanitization. #3

Merged

ChangeWeDer merged 1 commit into `ChangeWeDer:master` from `porcupineyhairs:master` on Nov 29, 2021

porcupineyhairs commented on Nov 21, 2021 • edited

Contributor

Vulnerability Report

Summary

There exists a path traversal vulnerability in the `/<path:url>/<path:filename>` route. This occurs as attacker controlled values are used directly in the `send_from_directory` call.

The vulnerability can be attributed to the following block of code.

BaiduWenkuSpider_flaskWeb/GetAll.py
Lines 697 to 700 in 1247944

```
697     @app.route("/<path:url>/<path:filename>")
698     def downloader(url,filename):
699         dirpath = os.path.join(app.root_path, url)  # 下载文件目录路径
700         return send_from_directory(dirpath, filename, as_attachment=True)  #
        as_attachment=True 一定要写，不然会变成打开，而不是下载
```

`os.path.join` call is not safe when used with untrusted input. It does not behave well when linux and windows file schemes are mixed and can lead to path traversal vulnerabilities.

Remediation

The code in this PR should fix the underlying issue.

GitHub Security Advisories

If possible, please could you create a GitHub Security Advisory for these findings?
When you use a GitHub Security Advisory, you can request a CVE identification number from GitHub. GitHub usually reviews the request within 72 hours, and the CVE details will be published after you make your security advisory public. Publishing a GitHub Security Advisory and a CVE will help notify the downstream consumers of your project, so they can update to the fixed version.

`[security] Path traversal due to incorrect input sanitization. ...` `5b4a928`

porcupineyhairs commented on Nov 22, 2021 — Contributor — Author

@ChangeWeDer ping

ChangeWeDer merged commit `fe9a39e` into `ChangeWeDer:master` on Nov 29, 2021

---

porcupineyhairs commented on Nov 30, 2021 — Contributor — Author

@ChangeWeDer Can you please request an advisory for these findings?

porcupineyhairs mentioned this pull request on May 4

Python : Flask Path Traversal Vulnerability github/securitylab#669

Closed

2 tasks

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants