

[New issue](#)[Jump to bottom](#)

[security] CVE-2020-8440, Unrestricted file upload #10

🔒 Closed

gwen001 opened this issue on Jan 19, 2020 · 2 comments

gwen001 commented on Jan 19, 2020 • edited

Description: controllers/page_apply.php in simplejobscript.com SJS <=1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.**Environment:**

Version: 1.64
OS: Ubuntu 16.10
Web server: Apache 2.4.18
PHP: 5.6.40
Database: MySQL 5.7.28
URL: /apply

Steps to Reproduce:

- 1/ Apply for a job and attach a PHP file as your resume
- 2/ Browse the upload directory `http://local.simplejobscript.net/uploads/cvs/`
- 3/ Run the PHP file

Additional information:

If you can't see the content of the upload directory (directory indexing is off), it can be hard to guess the final filename of your malicious resume because of the `uniqid` generated. However, you can use one of the multiple SQL injection ([CVE-2020-7229](#)) then read the content of the table `applicant` or use one of the multiples IDOR available to have access to all applications of all companies.

PoC:

The screenshot shows a web browser window with the address bar displaying `http://local.simplejobscript.net/uploads/cvs/`. The page title is "Index of /uploads/cvs". Below the title, there is a table with columns "Name", "Last modified", "Size", and "Description". The table lists several files, including `xphp_5e245460e23ce.php`, `xphp_5e2454494d3ae.php`, and `xphp_5e245418432dd.php`. Below the table, there is a code snippet for a PHP file named `xphp_5e245418432dd.php`. The code snippet shows a remote code execution payload using `eval` and `system` functions.

niteosoft commented on Jan 28, 2020

Ownerfixed in the last commit [d7c1b4b](#)🔒 niteosoft closed this as completed on Jan 28, 2020

gwen001 commented on Jan 28, 2020

Author

Perfect :)

gwen001 changed the title [security] Unrestricted file upload [security] CVE-2020-8440, Unrestricted file upload on Jan 29, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

