🐛 | Command Injection and XSS vulnerabilities reports #1859

Closed enferas opened this issue on Jul 18 · 3 comments · Fixed by #1862

Labels bug needs triage php

enferas commented on Jul 18 Contributor

Hello,

I would like to report for possible vulnerability.

In file https://github.com/MiczFlor/RPi-Jukebox-RFID/blob/develop/htdocs/trackEdit.php

```
//line 136
if(isset($_GET['folder']) && $_GET['folder'] != "") {
    $post['folder'] = $_GET['folder'];
} else {
    if(isset($_POST['folder']) && $_POST['folder'] != "") {
        $post['folder'] = $_POST['folder'];
    }
}
if(isset($_GET['filename']) && $_GET['filename'] != "") {
    $post['filename'] = $_GET['filename'];
} else {
    if(isset($_POST['filename']) && $_POST['filename'] != "") {
        $post['filename'] = $_POST['filename'];
    }
}
//line 249
$fileName = Files::buildPath($post['folder'], $post['filename']);
$exec = "mid3v2 -l '" .$fileName ."'" ;
```

In file https://github.com/MiczFlor/RPi-Jukebox-RFID/blob/develop/htdocs/utils/Files.php

```
public static function buildPath(...$pieces) {
        return implode(DIRECTORY_SEPARATOR, $pieces);
```

```
    }
```

So the attacker can control the command injection through the filename.
The attacker can add ';' and add another command like (echo <script>alert(document.cookie)<\script>.
The output pf the command will be printed through this path.

In file https://github.com/MiczFlor/RPi-Jukebox-RFID/blob/develop/htdocs/trackEdit.php

```
//line 252
// note: the output of the command is in $res
$lines = explode(PHP_EOL, $res);
foreach($lines as $line) {
    $parts = explode("=",$line);
    $key = trim(array_shift($parts)); // take the first
    $val = trim(implode("=",$parts)); // put the rest back together
    if (in_array($key, $trackDat['metaKeys']['mp3'])) {
        $trackDat['existingTags'][$key] = $val;
    }
}
//line 496
if (isset($trackDat['existingTags']['TCOM']) && trim($trackDat['existingTags']['TCOM']) != "") {
              echo trim($trackDat['existingTags']['TCOM']);
}
```

Finally, I recommend using escapeshellarg function with the $_GET['folder'], $_POST['folder'], $_GET['filename'] and $_POST['filename']

enferas added bug **needs triage** labels on Jul 18

s-martin added the **php** label on Jul 21

s-martin commented on Jul 21 Collaborator

Hi, thanks for pointing that out.

If you want to provide a pull request with the necessary changes it would also be appreciated :)

@MiczFlor

enferas mentioned this issue on Jul 23

Fix Command Injection and XSS vulnerabilities in trackEdit.php #1862

Merged

enferas commented on Jul 23 — Contributor — Author

Thank you for your response.
I sent the pull request.

❤️ 1

s-martin linked a pull request on Jul 24 that will close this issue

Fix Command Injection and XSS vulnerabilities in trackEdit.php #1862 — Merged

enferas commented on Sep 21 — Contributor — Author

CVE-2022-36749 is assigned for this report.

s-martin closed this as completed in #1862 on Oct 26

Assignees

No one assigned

Labels

bug needs triage php

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix Command Injection and XSS vulnerabilities in trackEdit.php
enferas/RPi-Jukebox-RFID

2 participants