OS COMMAND INJECTION IN LARAVEL FRAMEWORK

Title
OS Command Injection In Laravel Framework

Advisory ID
NBS-2021-0004

Product
Laravel Framework

Vulnerable Version
< 5.8.17

Fixed Version
5.8.17

CVE ID
CVE-2020-19316

Homepage
https://www.laravel.com/

Discovery Date
19 May 2019

Author
Ramadhan Amizudin | NetbyteSEC

Product description:

"Laravel is a web application framework with expressive, elegant syntax. We've already laid the foundation
— freeing you to create without sweating the small things."

Source : https://www.laravel.com/

Vulnerability description:

OS Command Injection found in Filesystem Symlink API (CVE-2020-19316) When passing crafted user input into the Storage::link() will trigger the vulnerability. Exploiting this issue may allow attacker to execute OS Command with running application privilege. This vulnerability affect laravel installation on the Windows operating system only.

Proof Of Concept:

For version 5.7.16
File: src/Illuminate/Filesystem/Filesystem.php
Line: 257

```
public function link($target, $link)
{
  if (! windows_os()) { // [1]
    return symlink($target, $link);
  }
  $mode = $this->isDirectory($target) ? 'J' : 'H';
  exec("mklink /{$mode} \"{$link}\" \"{$target}\""); // [2]
}
```

OS checking done at **[1]**, if the current OS is not windows the execution will continue.

Finally the variable reach **[2]** code path, which take variable into exec function without any escape.

Because the Filesystem API is mapped into Storage facade, we can demonstrate the vulnerability by using this vulnerable code in the controller

```
Storage::link($request->input('target_folder'), $request->input('link_name'));
```

Mitigation:

The vulnerability is patched on version 5.8.17 and above. Please update your laravel to the latest version.

Timeline:

2019-05-10 | Contact Laravel Security, (Taylor Otwell) via taylor[at]laravel.com
2019-05-14 | Laravel Version 5.8.17 released
2019-05-14 | Applied for CVE
2021-12-13 | CVE-2020-19316 Assigned
2021-12-16 | Advisory Published