fracpete / vfsjfilechooser2 Public

Code Issues 3 Pull requests Actions Projects Security ...

New issue

Jump to bottom

Vulnerable Regular Expression in vfsjfilechooser2 #7

Closed yetingli opened this issue on Sep 30, 2020 · 5 comments

yetingli commented on Sep 30, 2020

Type of Issue
Potential Regex Denial of Service (ReDoS)

Description
The vulnerable regular expression is located in

vfsjfilechooser2/src/main/java/com/googlecode/vfsjfilechooser2/utils/VFSURIValidator.java
Line 235 in 5a5f348

```
235      Pattern p_ftp2 = Pattern
```

The ReDOS vulnerability can be exploited with the following string
`ftp://:@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::`

You can execute the following code to reproduce ReDos

```
import com.googlecode.vfsjfilechooser2.utils.VFSURIValidator;

public class Main {
    public static void main(String[] args) {
        VFSURIValidator v = new VFSURIValidator();
        String _uri = "ftp://:@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::@::";
        System.out.println(v.isValid(_uri));
    }
}
```

I think you can limit the input length or modify this regex.

fracpete commented on Sep 30, 2020 Owner

This project hasn't been under active development for a number of years (I no longer use it). Propose a patch that mitigates the problem and I'll have a look at it.

yetingli commented on Oct 6, 2020 Author

> This project hasn't been under active development for a number of years (I no longer use it). Propose a patch that mitigates the problem and I'll have a look at it.

I am willing to suggest that you replace the Pattern p_ftp2 `(ftp|FTP|sftp|SFTP|http|HTTP|https|HTTPS|webdav|WEBDAV|smb|SMB)://(.+:.+@)*([^:]+?/*)([ ]*:[0-9]+)*([ ]*:)*(/.*)` with `(ftp|FTP|sftp|SFTP|http|HTTP|https|HTTPS|webdav|WEBDAV|smb|SMB)://([^:@]+:[^:@]+@)*([^:]+?/*)([ ]*:[0-9]+)*([ ]*:)*(/.*)`

Similarly, Pattern p_ftp3 can also be modified in this way.

Feel free to contact me if you have any questions on these vulnerability disclosures :).

fracpete added a commit that referenced this issue on Oct 6, 2020

`incorporated Yeting Li's fix for Potential Regex Denial of Service (R…` ··· `9c9f2c3`

fracpete commented on Oct 6, 2020 Owner

Thanks for that. Tested and incorporated the fix. Also fixed handling of specials chars in passwords, which need to be URL encoded. Pushed out a new release (0.2.9) to Maven Central.

👍 1

fracpete closed this as completed on Oct 6, 2020

OS-WS commented on Jun 22, 2021

Hi, Was CVE-2021-29061 fixed?
If so, in what commit/version?

Thanks!!

fracpete commented on Jun 22, 2021 Owner

0.2.9 as it says in the comment before your comment.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants