

Jump to bottom

Regular Expression DoS vulnerability in the gedit3 plugin #191



New issue

Open linci8210 opened this issue on May 29, 2020 · 1 comment

linci8210 commented on May 29, 2020

Regular Expression DoS vulnerability in the gedit3 plugin

We are working on the ReDoS problem and detected two vulnerable regexes from your gedit3 plugin code.

.+(<.+>)+([0-9]+)(<.+>)+.* in link

It takes forever for the regex to match the string

We suggest you change the structure (<.+>)+.*, since "." can accept "<" and ">".

Vulnerable regex 2:

 $</?[\w:-]+(?:\s+[\w-:]+(?:\s^*=\s^*(?:(?:"[^"]")|(?:'[^\']")|[^>\s]+))?)\setminus s(/?)>$

in link and link

This vulnerability can be triggered by

"<- -=\"\" -=\"\

We didn't create a pull request because we're not sure if these cases are possible to take place in your program, we also do not understand the functionality of these regexes as you do. Thank you for your understanding.

abergmann commented on Sep 23, 2021

CVE-2020-23469 was assigned to this issue.

No one assigned

Projects

Milestone

No branches or pull requests

2 participants

