

New issue

[Jump to bottom](#)

[SECURITY] Denial of service because of unsafe regex processing #8680

🔒 Closed ghost opened this issue on Jun 10, 2021 · 10 comments · Fixed by #8751

Labels enhancement security

ghost commented on Jun 10, 2021

I have tried to contact you by cbiportal@cbio.mskcc.org and asked for any other email in #8658. Nobody replied.

The cBioPortal is vulnerable to regex injection that may lead to Denial of Service.

User controlled heatmap and alteration are used to build and run a regex expression:

[cbiportal/core/src/main/java/org/mskcc/cbio/portal/servlet/ProteinArraySignificanceTestJSON.java](#)
Lines 104 to 106 in e86d40

```
104 String heatmap = request.getParameter("heat_map");
105 String gene = request.getParameter("gene");
106 String alterationType = request.getParameter("alteration");
```

The value end up in getAlteredCases

[cbiportal/core/src/main/java/org/mskcc/cbio/portal/servlet/ProteinArraySignificanceTestJSON.java](#)
Lines 279 to 282 in e86d40

```
279 if (parts[1].equals(alterationType)
280     || parts[1].matches("^"+alterationType+"[;\\t]")
281     || parts[1].matches("."+[;\\t]+alterationType+"[;\\t]")
282     || parts[1].matches("."+[;\\t]+alterationType+"$")) {
```

Since the attacker controls the string and the regex pattern he may cause a ReDoS by regex catastrophic backtracking on the server side.

inodb commented on Jun 15, 2021

Member

CC @adamabeshouse

🏷️ inodb added the security label on Jun 15, 2021

inodb commented on Jun 15, 2021

Member

Thanks for reporting! I don't think this code is used anymore actually? Maybe we can delete it?

🔒 jjgao closed this as completed on Jun 22, 2021

ghost commented on Jun 28, 2021

Author

Hi,
Do you plan to release a GitHub security advisory and/or request CVE number?

ghost commented on Jun 28, 2021

Author

Oh, did you just close the issue without fixing the code? Even if the parameters are not used the code is still callable. Do I miss something?

ghost commented on Jul 13, 2021

Author

I thought since the issue was so brutally closed without explanation maybe my code analysis is wrong and it is not exploitable. Thus I have followed the instructions from <https://docs.cbioportal.org/2.1.1-deploy-with-docker-recommended/docker> and ran a local instance of cbiportal in container. I have a proof of concept when just a single request makes server cpu to consume 100% indefinitely. Please create a [security advisory](#) where you could invite me and discuss it in private if you have any questions.

It makes me sad that such a noble project makes it hard to responsibly disclose a security issue that may potentially lead to Denial of Service. Please respond in 24 hours.

jjgao commented on Jul 15, 2021 • edited

Member

@edvraa Thanks for reporting this. The code is not being used in production anymore. Also, we planned to retire both core and portal modules once all dependencies are removed ([cBioPortal/icebox#161](#)), so at this moment, we will not invest time fixing issues in these two modules that will not be running in production.

ghost commented on Jul 15, 2021 • edited by ghost


Author

@jjgao The question is not if it is used or not. Single request to http://cbiportal1.org/ProteinArraySignificanceTest.json?heat_map=censored&gene=censored&alteration=censored will make the web server consume 100% CPU. Multiple requests like this may potentially take down the server. Since it is not used, commenting out the function or disabling the route sounds as easy fix, right?

 **adamabeshouse** mentioned this issue on Jul 15, 2021

Delete unused ProteinArraySignificanceTest endpoint with security issue #8751

→ Merged

 **sheridancbio** added the **enhancement** label on Jul 15, 2021

adamabeshouse commented on Jul 20, 2021

Contributor

@edvraa thanks for reporting this! The endpoint has now been deleted in master.

ghost commented on Jul 20, 2021


Author

A pity it didn't make it into <https://github.com/cBioPortal/cbioportal/releases/tag/v3.6.21> by one hour.

adamabeshouse commented on Jul 20, 2021 • edited

Contributor

We release frequently and it will be in the next one.

 **ghost** mentioned this issue on Aug 18, 2021

Java: **Regex injection** [github/securitylab#423](#)

🔒 Closed

Assignees

No one assigned

Labels

enhancement **security**

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

🔗 Delete unused ProteinArraySignificanceTest endpoint with security issue
cBioPortal/cbioportal

4 participants

