21

[idp.fr.cloud.gov] Open Redirect

Share:

State	○ Resolved (Closed)
Disclosed	**November 1, 2018 7:49pm +0100**
Reported To	TTS Bug Bounty
Asset	https://idp.fr.cloud.gov (Domain)
Weakness	Open Redirect
Bounty	$150
Severity	Low (3.8)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

bobrov submitted a report to **TTS Bug Bounty**. Jul 26th (about 1 year ago)

Description: Open Redirect

Domain: idp.fr.cloud.gov

Steps To Reproduce:
Open URL:

```
https://idp.fr.cloud.gov//blackfan.ru/..;/css
```

HTTP Response

```
HTTP/1.1 302 Found
...
Location: //blackfan.ru/..;/css/
...
```

Impact

A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

glassofbeer HackerOne staff posted a comment. Jul 27th (about 1 year ago)

@bobrov

Thanks for your submission. We will review it and get back to you.

Best Regards.

glassofbeer HackerOne staff updated the severity from Low to Low (3.8). Jul 27th (about 1 year ago)

glassofbeer HackerOne staff changed the status to ○ **Triaged**. Jul 31st (12 months ago)

Hey @bobrov

Thank you for your submission. We have validated this issue and forwarded the report to the responsible team for this application. They will evaluate and let us know whether or not they will be implementing a fix.

Thanks!

TTS Bug Bounty rewarded bobrov with a **$150** bounty. Aug 21st (11 months ago)

After reviewing your submission, it was determined that this issue is eligible for a bounty. We are issuing you a $150 bounty for this `Low` -severity issue.

Thank you once again for your report and we look forward to working with you again in the near future.

bobrov posted a comment. Oct 10th (10 months ago)

Most likely this is

Apache Tomcat Open Redirect CVE-2018-11784
https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.12

Mitigation
Users of the affected versions should apply one of the following
mitigations:

Upgrade to Apache Tomcat 9.0.12 or later.
Upgrade to Apache Tomcat 8.5.34 or later.
Upgrade to Apache Tomcat 7.0.91 or later.
Use mapperDirectoryRedirectEnabled="true" and mapperContextRootRedirectEnabled="true" on the Context to ensure that redirects are issued by the Mapper rather than the default Servlet. See the Context configuration documentation for further important details.

adamkendallgsa posted a comment. Oct 10th (10 months ago)

@bobrov Thanks for the original report, and for following up. We recently deployed the upgrade necessary to close this issue, and your proof of concept now returns a 404 as expected.

coffeecup HackerOne staff closed the report and changed the status to ○ **Resolved**. Oct 12th (10 months ago)

Hello,

Thanks for submitting this report. We have determined that this report is now resolved. If you’re still able to reproduce this issue, please let us know and we will investigate further.

Thanks!

bobrov requested to disclose this report. Oct 19th (9 months ago)

britta agreed to disclose this report. Nov 1st (9 months ago)

We consider the details of this report non-sensitive, so we're agreeing to publicly disclose it as requested by the reporter. Thanks @bobrov!

This report has been disclosed. Nov 1st (9 months ago)