

58

Identity Login Page Redirect Can Be Manipulated

Share:      

State

Resolved (Closed)

Disclosed

October 13, 2017 6:15pm +0200

Reported To

Inflection

Asset

www.identity.com
(Domain)

Weakness

Open Redirect



Bounty

\$750

Severity

High (8.1)

Participants

Visibility

Disclosed (Limited)

Collapse

SUMMARY BY INFLECTION



The Identity.com login page could be manipulated to redirect the user to an arbitrary URL after a successful authentication.

Researcher POC

- I used this request to try login https://www.identity.com/signin?redirect_url=%2Foauth%2Fauthorize%3Fclient_id%3D241f887e145f09298fc7f3459cefa080cd7abd30b7b0192977b5bb72965e0583%26redirect_uri%3D%252Ftest-callback%26response_type%3Dcode%26scope%3Dname%2Bemail%2Bdob%26state%3DAPPLICATION_TEST
- I put %40google.com after redirect_url= so the endpoint was like this
&redirect_url=%40google.com%2Fclient_id%253D241f887e145f09298fc7f3459cefa080cd7abd30b7b0192977b5bb72965e0583%2526redirect_uri%253D%25252Ftest-callback%2526response_type%253Dcode%2526scope%253Dname%252Bemail%252Bdob%2526state%253DAPPLICATION_TEST
- After a successfully login i redirect to google.com

TIMELINE · EXPORT



- malcolmx submitted a report to [Inflection](#).

Jun 27th (2 years ago)
- mmuller-inflection updated the severity.

Jun 27th (2 years ago)
- mmuller-inflection changed the report title.

Jun 27th (2 years ago)
- mmuller-inflection changed the status to Triaged.

Jun 27th (2 years ago)
- Inflection rewarded malcolmx with a \$750 bounty.

Jun 27th (2 years ago)
- malcolmx posted a comment.

Jun 27th (2 years ago)
- malcolmx posted a comment.

Jun 28th (2 years ago)
- malcolmx posted a comment.

Jun 29th (2 years ago)
- mmuller-inflection posted a comment.

Jun 29th (2 years ago)
- malcolmx posted a comment.

Jun 29th (2 years ago)
- mmuller-inflection closed the report and changed the status to Resolved.

Jul 12th (2 years ago)

<div><div></div><div>malcolmx requested to disclose this report.</div></div>	Oct 13th (2 years ago)
<div><div></div><div>mmuller-inflection agreed to disclose this report.</div></div>	Oct 13th (2 years ago)
<div><div></div><div>This report has been disclosed.</div></div>	Oct 13th (2 years ago)
<div><div></div><div>mmuller-inflection changed the scope from None to www.identity.com.</div></div>	Oct 31st (2 years ago)