

19

Open redirect at app.goodhire.com via returnUrl parameter

Share:



State

Resolved (Closed)

Disclosed

February 21, 2018 8:37pm +0100

Reported To

Inflection

Asset

app.goodhire.com
(Domain)

Weakness

None



Bounty

\$750

Severity

High (7.4)

Participants




Visibility

Disclosed (Limited)


Collapse

SUMMARY BY INFLECTION




At login, the returnUrl parameter could be manipulated to send a user to any arbitrary URL, rather than just a local redirect, if the user was already logged into their GoodHire account and visited the login page again.


TIMELINE · EXPORT

- 


exception submitted a report to Inflection.

Jun 15th (2 years ago)
- 


exception posted a comment.

Jun 15th (2 years ago)
- 


mmuller-inflection changed the status to Needs more info.

Jun 15th (2 years ago)
- 


exception changed the status to New.

Jun 15th (2 years ago)
- 


mmuller-inflection updated the severity.

Jun 15th (2 years ago)
- 


mmuller-inflection changed the status to Triaged.

Jun 15th (2 years ago)
- 


Inflection rewarded exception with a \$750 bounty.

Jun 15th (2 years ago)
- 


mmuller-inflection closed the report and changed the status to Resolved.

Jun 29th (2 years ago)
- 


mmuller-inflection changed the scope from None to app.goodhire.com.

Oct 31st (2 years ago)
- 

exception requested to disclose this report.

Feb 20th (about 1 year ago)
- 

mmuller-inflection agreed to disclose this report.

Feb 21st (about 1 year ago)
- 

This report has been disclosed.

Feb 21st (about 1 year ago)