

29

Exploiting Misconfigured CORS to Steal User Information

Share:



State

Resolved (Closed)

Disclosed

October 17, 2018 5:04pm +0200

Reported To

Rockstar Games

Asset

www.rockstargames.com
(Domain)

Weakness

Information Disclosure


Bounty

\$500

Severity

High (7 ~ 8.9)

Participants



Visibility

Disclosed (Limited)

Collapse

SUMMARY BY ROCKSTAR GAMES



In this report, the researcher demonstrated how a CORS misconfiguration was allowing user details, such as email addresses and IDs, to be shared inappropriately. They also provided a POC which showed how an attacker could exploit this remotely. This issue was resolved in a platform update to our Support site; the gateway that was leaking user information was removed entirely.

TIMELINE · EXPORT



- 1hack0 submitted a report to Rockstar Games.

Feb 18th (about 1 year ago)
- jmarshall changed the status to Triaged.

Feb 19th (about 1 year ago)
- 1hack0 posted a comment.

Feb 26th (about 1 year ago)
- jmarshall posted a comment.

Feb 28th (about 1 year ago)
- Rockstar Games rewarded 1hack0 with a \$500 bounty.

Feb 28th (about 1 year ago)
- 1hack0 posted a comment.

Updated Mar 5th (about 1 year ago)
- jmarshall posted a comment.

Mar 5th (about 1 year ago)
- jmarshall closed the report and changed the status to Resolved.

Oct 17th (10 months ago)
- 1hack0 requested to disclose this report.

Oct 17th (10 months ago)
- jmarshall posted a comment.

Oct 17th (9 months ago)
- jmarshall agreed to disclose this report.

Oct 17th (9 months ago)
- This report has been disclosed.

Oct 17th (9 months ago)
- 1hack0 posted a comment.

Jan 9th (7 months ago)
- 1hack0 posted a comment.

Jan 9th (7 months ago)

