

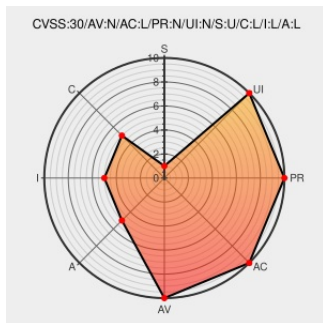


CVE-2018-10966

Published on: 06/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10966

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Gamerpolls](#) from [Gamerpolls](#) contain the following vulnerability:

An issue was discovered in GamerPolls 0.4.6, related to config/environments/all.js and config/initializers/02_passport.js. An attacker can edit the Passport.js contents of the session cookie to contain the ID number of the account they wish to take over, and re-sign it using the hard coded secret.

CVE-2018-10966 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	LOW	LOW

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Remove use of hard coded secret by rastating · Pull Request #56 · GamerPolls/gamerpolls.com · GitHub	Patch Third Party Advisory github.com	MISC github.com/GamerPolls/gamerpolls.com/pull/56

text/html

Continuous Cyber Security | UK | Digital Interruption

ExploitThird Party Advisoryweb.archive.orgtext/htmlInactive LinkNot Archived

gamerpolls.com/all.js at 03ccbf219410e0a45390d0efc12017f08a25282 · GamerPolls/gamerpolls.com · GitHub

PatchThird Party Advisorygithub.comtext/html

CONFIRMgithub.com/GamerPolls/gamerpolls.com/blob/03ccbf219410e0a45390d0efc12017f08a25282

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gamerpolls	Gamerpolls	0.4.6	All	All	All
Application	Gamerpolls	Gamerpolls	0.4.6	All	All	All

cpe:2.3:a:gamerpolls:gamerpolls:0.4.6:*:*:*:*:*:

cpe:2.3:a:gamerpolls:gamerpolls:0.4.6:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →