



CVE-2018-12975

Published on: 09/24/2018 12:00:00 AM UTC

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

CVE-2018-12975

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

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

The random() function of the smart contract implementation for CryptoSaga, an Ethereum game, generates a random value with publicly readable variables such as timestamp, the current block's blockhash, and a private variable (which can be read with a `getStorageAt` call). Therefore, attackers can precompute the random number and manipulate the game (e.g., get powerful characters or get critical damages).

CVE-2018-12975 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Create legendary champs by breaking PRNG of Cryptosaga, an Ethereum RPG game (CVE-2018-12975)	Exploit Third Party Advisory	MISC medium.com/@jonghyk.song/create-legendary-champs-by-breaking-prng-of-cryptosaga-an-

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	Cryptosaga	Cryptosaga	-	All	All	All
Application	Cryptosaga	Cryptosaga	-	All	All	All
cpe:2.3:a:cryptosaga:cryptosaga:-:*:*:*:*:*:						
cpe:2.3:a:cryptosaga:cryptosaga:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)