

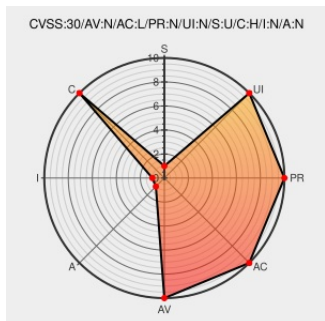


CVE-2018-14715

Published on: 08/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-14715

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

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

The endCoinFlip function and throwSlammer function of the smart contract implementations for Cryptogs, an Ethereum game, generate random numbers with an old block's hash. Therefore, attackers can predict the random number and always win the game.

CVE-2018-14715 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
Attack on Pseudo-random number generator(PRNG) used in Cryptogs, an Ethereum (CVE-2018-14715) by Jonghyuk Song Coinmonks Medium	Exploit Third Party Advisory medium.com text/html	MISC medium.com/@jonghyk.song/attack-on-pseudo-random-number-generator-prng-used-in-cryptogs-an-ethereum-cve-2018-14715-f63a51ac2eb9

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	Cryptogs	Cryptogs	-	All	All	All
Application	Cryptogs	Cryptogs	-	All	All	All
cpe:2.3:a:cryptogs:cryptogs:-:*:*:*:*:*:						
cpe:2.3:a:cryptogs:cryptogs:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)