

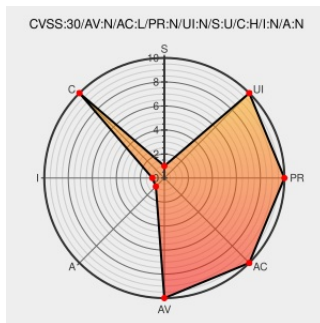


CVE-2018-17968

Published on: 10/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:20 PM UTC

CVE-2018-17968

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

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

A gambling smart contract implementation for Ruletkalo, an Ethereum gambling game, generates a random value that is predictable by an external contract call. The developer wrote a random() function that uses a block timestamp and block hash from the Ethereum blockchain. This can be predicted by writing the same random function code in an exploit contract to determine the deadSeat value.

CVE-2018-17968 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
CVE-LIST/CVE-2018-17968 at master · TEAM-C4B/CVE-LIST · GitHub	Exploit Third Party Advisory	MISC github.com/TEAM-C4B/CVE-LIST/tree/master/CVE-2018-17968

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	Ruletikaio	Ruletikaio	-	All	All	All
Application	Ruletikaio	Ruletikaio	-	All	All	All
cpe:2.3:a:ruletikaio:ruletikaio:-:*:*:*:*:*:						
cpe:2.3:a:ruletikaio:ruletikaio:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)