



CVE-2018-13547

Published on: 07/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-13547

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

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

The mintToken function of a smart contract implementation for Providence Crypto Casino (PVE) (Contract Name: ProvidenceCasinoToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.

CVE-2018-13547 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	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
EtherTokens/ProvidenceCasinoToken at master · BlockChainsSecurity/EtherTokens · GitHub	Third Party Advisory github.com text/html	MISC github.com/BlockChainsSecurity/EtherTokens/tree/master/Providence

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pve Project	Pve	-	All	All	All
Application	Pve Project	Pve	-	All	All	All
cpe:2.3:a:pve_project:pve:-:*:*:*:*:*:						
cpe:2.3:a:pve_project:pve:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Next ID→