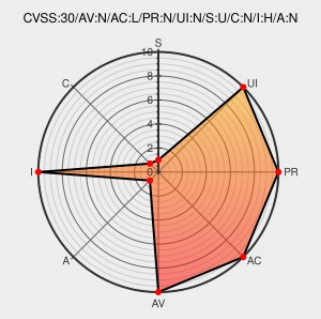
CVE-2018-13758

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

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

CVE-2018-13758

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Lolicoin from Lolicoin Project contain the following vulnerability:

The mintToken function of a smart contract implementation for LoliCoin, 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-2018-13758 has been assigned by 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/LoliCoin at master · BlockChainsSecurity/EtherTokens · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/BlockChainsSecurity/EtherTokens/tree/master/LoliCoin
EtherTokens/mint integer	Exploit	MISC

overflow.md at master · BlockChainsSecurity/EtherTokens · GitHub	Third Party Advisory github.com text/html	github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20int

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lolicoin Project	Lolicoin	-	All	All	All
Application	Lolicoin Project	Lolicoin	-	All	All	All

cpe:2.3:a:lolicoin_project:lolicoin:-:*:*:*:*:*:*:*:

cpe:2.3:a:lolicoin_project:lolicoin:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→