



CVE-2018-13765

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

Last Modified on: 03/23/2021 11:24:29 PM UTC

CVE-2018-13765

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The mintToken function of a smart contract implementation for LandCoin, 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-2018-13765 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/LandCoin at master · BlockChainsSecurity/EtherTokens · GitHub	Third Party Advisory github.com text/html	MISC github.com/BlockChainsSecurity/EtherTokens/tree/master/LandCoin

 MISC
github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20int

◀ ▶

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report