



CVE-2018-13678

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-13678
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-09 06:29:00 UTC
Updated	2018-07-19 15:43:00 UTC
Description	The mintToken function of a smart contract implementation for Lottery, an Ethereum token, has an integer overflow that allc

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
EtherTokens/Lottery at master · BlockChainsSecurity/EtherTokens · GitHub	MISC	github.com	Third Party Advis
EtherTokens/mint integer overflow.md at master · BlockChainsSecurity/EtherTokens · GitHub	MISC	github.com	Exploit, Third Par
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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