



CVE-2018-18667

Published on: 12/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

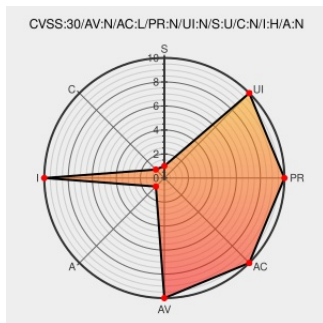
CVE-2018-18667

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: PDF



Certain versions of [Pylontoken](#) from [Pylon-network](#) contain the following vulnerability:

The mintToken function of Pylon (PYLNT) aka PylonToken, 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, a related issue to CVE-2018-11812.

CVE-2018-18667 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
PylonToken 0x7703c35cffdc5cda8d27aa3df2f9ba6964544b6e	Third Party Advisory etherscan.io text/html	MISC etherscan.io/address/0x7703c35cffdc5cda8d27aa3df2f9ba6964544
smart_contract_-vulnerability/PolyAi.md at	Exploit	MISC github.com/n0pn0pn0p/smart_contract_-

master · n0pn0pn0p/smart_contract_ - vulnerability · GitHub

Third Party Advisory

github.com

text/html

vulnerability/blob/master/PolyAi.md

a overflow vulnerability in mintToken · Issue #1 · klenergy/ethereum-contracts · GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC github.com/klenergy/ethereum-contracts/issues/1

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	Pylon-network	Pylontoken	-	All	All	All
Application	Pylon-network	Pylontoken	-	All	All	All

cpe:2.3:a:pylon-network:pylontoken:-:*:*:*:*:*:

cpe:2.3:a:pylon-network:pylontoken:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →