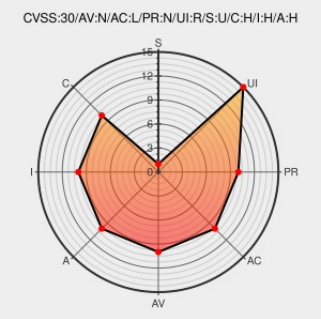
CVE-2018-18920

Published on: 11/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18920

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



Certain versions of Py-evm from Ethereum contain the following vulnerability:

Py-EVM v0.2.0-alpha.33 allows attackers to make a vm.execute_bytecode call that triggers computation._stack.values with '"stack": [100, 100, 0]' where b'\x' was expected, resulting in an execution failure because of an invalid opcode. This is reportedly related to "smart contracts can be executed indefinitely without gas being paid."

CVE-2018-18920 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
JavaScript is not available.	Third Party Advisory nitter.domain.glass	MISC twitter.com/NettaLab/status/1060889400102383617

	text/html	
vbuterin comments on Netta labs claim to have found a vulnerability in EVM, what are your thoughts?	Third Party Advisory www.reddit.com text/html	MISC www.reddit.com/r/ethereum/comments/9vkk2g/netta_labs_claim_to_have_found_a_vulner
Invalid values like 100, 0 occurs in Stack during the execution. · Issue #1448 · ethereum/py-evm · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/ethereum/py-evm/issues/1448
Alex.eth na Twitterze: "@VitalikButerin just commented on this via reddit: https://t.co/EoKMDdykzq… "	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/AlexanderFisher/status/1060923428641878019

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.

Related QID Numbers

980839 Python (pip) Security Update for py-evm (GHSA-vqgp-4jgj-5j64)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ethereum	Py-evm	0.2.0	alpha.33	All	All
Application	Ethereum	Py-evm	0.2.0	alpha.33	All	All

cpe:2.3:a:ethereum:py-evm:0.2.0:alpha.33:*:*:*:*:*:*:

cpe:2.3:a:ethereum:py-evm:0.2.0:alpha.33:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→