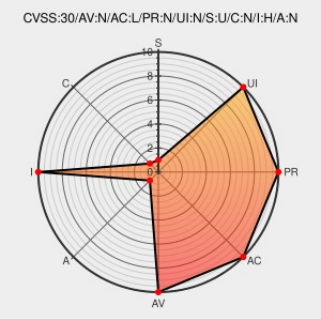
CVE-2019-7167

Published on: 03/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-7167

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



Certain versions of Zcash from Z.cash contain the following vulnerability:

Zcash, before the Sapling network upgrade (2018-10-28), had a counterfeiting vulnerability. A key-generation process, during evaluation of polynomials related to a to-be-proven statement, produced certain bypass elements. Availability of these elements allowed a cheating prover to bypass a consistency check, and consequently transform the proof of one statement into an ostensibly valid proof of a different statement, thereby breaking the soundness of the proof system. This misled the original Sprout zk-SNARK verifier into accepting the correctness of a transaction.

CVE-2019-7167 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

GitHub - JinBean/CVE-Extension: This repository is an extension of our research on cryptocurrency clones and documents existing vulnerabilities discovered in those clones	github.com text/html	MISC github.com/JinBean/CVE-Extension
Zcash Counterfeiting Vulnerability Successfully Remediated - Electric Coin Company	Vendor Advisory z.cash text/html	MISC z.cash/blog/zcash-counterfeiting-vulnerability-successfully-remediated/
Zcash Bug Could Have Allowed 'Infinite Counterfeit' Cryptocurrency | Fortune	Press/Media Coverage Third Party Advisory fortune.com text/html	MISC fortune.com/2019/02/05/zcash-vulnerability-cryptocurrency/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Z.cash	Zcash	All	All	All	All

cpe:2.3:a:z.cash:zcash:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@zooko	Read this interesting backstory, which also mentions the BCTV14 flaw that led to CVE-2019-7167: hackmd.io/@omershlo/Sk_8…	2021-12-14 16:39:18
@zooko	Here's the full details on CVE-2019-7167: electriccoin.co/blog/zcash-cou…	2021-12-14 16:39:34

← Previous ID

Next ID→