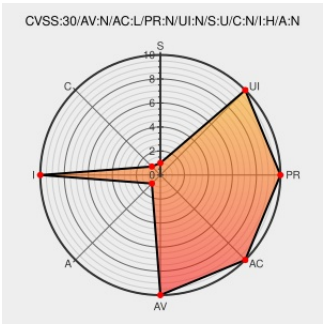
CVE-2018-10831

Published on: 05/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10831

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



Certain versions of Z-nomp from Zclassic contain the following vulnerability:

Z-NOMP before 2018-04-05 has an incorrect Equihash solution verifier that allows attackers to spoof mining shares, as demonstrated by providing a solution with {x1=1,x2=1,x3=1,...,x512=1} to bypass this verifier for any blockheader. This originally affected (for example) the Bitcoin Gold and Zcash cryptocurrencies, and continued to be exploited in the wild in May 2018 against smaller cryptocurrencies.

CVE-2018-10831 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
Update for the Equihash Mining	Third Party Advisory blog.zencash.com	MISC blog.zencash.com/update-for-the-equihash-mining-application-z-nomp/

Application Z-NOMP - Horizen	text/html	
misc/Attackers Fake Computational Power to Steal Cryptocurrencies from Mining Pools.md at master · edwardz246003/misc · GitHub	Exploit Technical Description Third Party Advisory github.com text/html	MISC github.com/edwardz246003/misc/blob/master/Attackers%20Fake%20Computational%20Power

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	Zclassic	Z-nomp	All	All	All	All

cpe:2.3:a:zclassic:z-nomp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→