



CVE-2022-34632

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

Summary

CVE	CVE-2022-34632
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-18 23:15:00 UTC
Updated	2022-07-26 18:14:00 UTC
Description	Rocket-Chip commit 4f8114374d8824dfdec03f576a8cd68bebce4e56 was discovered to contain insufficient cryptography vi

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Rocket Chip Generator	-	All	All	All

References

Reference
Zk(Zbk, Zkn, Zks)/Zb: Scalar Cryptography/Bitmanip Extension by ZenithalHourlyRate · Pull Request #2950 · chipsalliance/rocket-chip · GitHub
Zk(Zbk, Zkn, Zks)/Zb: Scalar Cryptography/Bitmanip Extension by ZenithalHourlyRate · Pull Request #2950 · chipsalliance/rocket-chip · GitHub
Zk(Zbk, Zkn, Zks)/Zb: Scalar Cryptography/Bitmanip Extension by ZenithalHourlyRate · Pull Request #2950 · chipsalliance/rocket-chip · GitHub
CVE Program record
NVD vulnerability detail

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