CVE-2017-9230

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-9230
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-24 16:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	The Bitcoin Proof-of-Work algorithm does not consider a certain attack methodology related to 80-byte block headers with a

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-338 | n/a | CWE-338 CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bitcoin	Bitcoin	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
ADP	Bitcoin	Bitcoin	affected -	Not specified

References

Reference	Source	Link
www.mit.edu/~jlrubin//public/pdfs/Asicboost.pdf	af854a3a-2127-422b-91ae-364da2661108	www.mit.edu
[bitcoin-dev] Treating ‘ASICBOOST’ as a Security Vulnerability	af854a3a-2127-422b-91ae-364da2661108	lists.linuxfoun
[bitcoin-dev] Treating ‘ASICBOOST’ as a Security Vulnerability	af854a3a-2127-422b-91ae-364da2661108	lists.linuxfoun
[bitcoin-dev] Treating ‘ASICBOOST’ as a Security Vulnerability	af854a3a-2127-422b-91ae-364da2661108	lists.linuxfoun
Bitcoin Proof-of-Work Algorithm CVE-2017-9230 Security Weakness	af854a3a-2127-422b-91ae-364da2661108	www.security
arxiv.org/ftp/arxiv/papers/1604/1604.00575.pdf	af854a3a-2127-422b-91ae-364da2661108	arxiv.org
[bitcoin-dev] BIP proposal: Inhibiting a covert attack on the Bitcoin POW function	af854a3a-2127-422b-91ae-364da2661108	lists.linuxfoun
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.