CVE-2008-5162

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

Summary

CVE	CVE-2008-5162
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-26 23:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The arc4random function in the kernel in FreeBSD 6.3 through 7.1 does not have a proper entropy source for a short time p

Risk And Classification

Primary CVSS: v3.1 7 HIGH from nvd@nist.gov

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

Problem Types: CWE-330 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.9		AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	6.3	-	All	All
Operating System	Freebsd	Freebsd	6.3	p1	All	All
Operating System	Freebsd	Freebsd	6.3	p2	All	All
Operating System	Freebsd	Freebsd	6.3	p3	All	All
Operating System	Freebsd	Freebsd	6.3	p4	All	All
Operating System	Freebsd	Freebsd	6.3	p5	All	All
Operating System	Freebsd	Freebsd	7.0	-	All	All
Operating System	Freebsd	Freebsd	7.0	p1	All	All
Operating System	Freebsd	Freebsd	7.0	p3	All	All
Operating System	Freebsd	Freebsd	7.0	p4	All	All
Operating System	Freebsd	Freebsd	7.0	p5	All	All
Operating System	Freebsd	Freebsd	7.1	-	All	All
Operating System	Freebsd	Freebsd	7.1	p1	All	All
Operating System	Freebsd	Freebsd	7.1	p10	All	All
Operating System	Freebsd	Freebsd	7.1	p12	All	All
Operating System	Freebsd	Freebsd	7.1	p13	All	All

Operating System	Freebsd	Freebsd	7.1	p14	All	All
Operating System	Freebsd	Freebsd	7.1	p15	All	All
Operating System	Freebsd	Freebsd	7.1	p16	All	All
Operating System	Freebsd	Freebsd	7.1	p2	All	All
Operating System	Freebsd	Freebsd	7.1	p3	All	All
Operating System	Freebsd	Freebsd	7.1	p4	All	All
Operating System	Freebsd	Freebsd	7.1	p5	All	All
Operating System	Freebsd	Freebsd	7.1	p6	All	All
Operating System	Freebsd	Freebsd	7.1	p7	All	All
Operating System	Freebsd	Freebsd	7.1	p8	All	All
Operating System	Freebsd	Freebsd	7.1	p9	All	All
Operating System	Freebsd	Freebsd	7.1	rc1	All	All
Operating System	Freebsd	Freebsd	7.1	rc2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
FreeBSD 'arc4random (9)' Pseudo-Random Number Generator Insufficient Entropy Weakness	af854a3a-2127-422b-91ae-364da2661108
osvdb.org/50137	af854a3a-2127-422b-91ae-364da2661108
FreeBSD "arc4random()" Insufficient Entropy Sources Security Issue - Secunia.com	af854a3a-2127-422b-91ae-364da2661108
security.freebsd.org/advisories/FreeBSD-SA-08:11.arc4random.asc	af854a3a-2127-422b-91ae-364da2661108
SecurityTracker.com Archives - FreeBSD arc4random(9) Generates Predictable Sequences	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**