# CVE Detail – CVE-2008-5162

The arc4random function in the kernel in FreeBSD 6.3 through 7.1 does not have a proper entropy source for a short time period immediately after boot, which makes it easier for attackers to predict the function's return values and conduct certain attacks against the GEOM framework and various network protocols, related to the Yarrow random number generator.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.19812

## CVSS Scoring

CVSS v3.1 Score: 7.0

Severity: HIGH

## Mapped CWE(s)

* CWE-330: Use of Insufficiently Random Values

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-485: Signature Spoofing by Key Recreation
* CAPEC-59: Session Credential Falsification through Prediction

## ATT&CK Techniques

* T1552.004: Private Keys
* T1110: Brute Force

## Used By (Actors/Tools)

* Machete (malware)
* Mafalda (malware)
* Hildegard (malware)
* Chaos (malware)
* FoggyWeb (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* QakBot (malware)
* jRAT (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Mimikatz (tool)
* CrackMapExec (tool)
* Operation Wocao (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* Volt Typhoon (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:o:freebsd:freebsd:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:p1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:p2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:p3:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:p4:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:6.3:p5:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.0:p1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.0:p3:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.0:p4:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.0:p5:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p10:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p12:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p13:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p14:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p15:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p16:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p3:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p4:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p5:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p6:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p7:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p8:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:p9:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:rc1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:freebsd:freebsd:7.1:rc2:\*:\*:\*:\*:\*:\*