



CVE-2003-1230

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1230

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Freebsd](#) from [Freebsd](#) contain the following vulnerability:

The implementation of SYN cookies (syncookies) in FreeBSD 4.5 through 5.0-RELEASE-p3 uses only 32-bit internal keys when generating syncookies, which makes it easier for remote attackers to conduct brute force ISN guessing attacks and spoof legitimate traffic.

CVE-2003-1230 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

[OSVDB 19785](#)

Inactive Link **Not Archived**

Secunia - Advisories - FreeBSD SYN cookie brute forcing

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[SECUNIA 8142](#)

FreeBSD syncookies TCP Initial Sequence Number Weakness

[Patch](#)

[cve.report \(archive\)](#)

[text/html](#)

[BID 6920](#)

SecurityFocus HOME Advisories: syncookies

[Patch](#)

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[FREEBSD FreeBSD-SA-03:03](#)

Inactive Link **Not Archived**

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

 **XF** [freebsd-syncookie-brute-force\(11397\)](#)

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
Operating System	Freebsd	Freebsd	4.5	release	All	All
Operating System	Freebsd	Freebsd	4.6	release	All	All
Operating System	Freebsd	Freebsd	4.7	release	All	All
Operating System	Freebsd	Freebsd	4.7	stable	All	All
Operating System	Freebsd	Freebsd	5.0	release	All	All
Operating System	Freebsd	Freebsd	4.5	release	All	All
Operating System	Freebsd	Freebsd	4.6	release	All	All
Operating System	Freebsd	Freebsd	4.7	release	All	All
Operating System	Freebsd	Freebsd	4.7	stable	All	All
Operating System	Freebsd	Freebsd	5.0	release	All	All

cpe:2.3:o:freebsd:freebsd:4.5:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.6:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.7:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.7:stable:****.*.*:

cpe:2.3:o:freebsd:freebsd:5.0:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.5:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.6:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.7:release:****.*.*:

cpe:2.3:o:freebsd:freebsd:4.7:stable:*.***.***.:

cpe:2.3:o:freebsd:freebsd:5.0:release:*.***.***.:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)