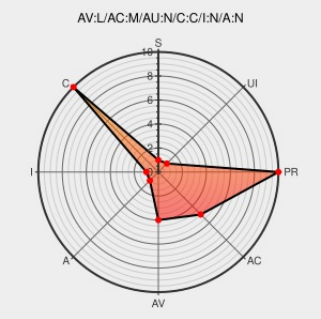
# CVE-2013-5666

Published on: 09/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

## CVE-2013-5666

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Freebsd from Freebsd contain the following vulnerability:

The sendfile system-call implementation in sys/kern/uipc_syscalls.c in the kernel in FreeBSD 9.2-RC1 and 9.2-RC2 does not properly pad transmissions, which allows local users to obtain sensitive information (kernel memory) via a length greater than the length of the file.

CVE-2013-5666 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 4.7 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| | Vendor Advisory, www.freebsd.org, text/plain | FREEBSD FreeBSD-SA-13:11 |
| FreeBSD Kernel sendfile(2) Discloses Kernel Memory Contents to Local Users - SecurityTracker | www.securitytracker.com, text/html | SECTRACK 1029013 |
| No Description Provided | osvdb.org, Inactive Link, Not Archived | OSVDB 97142 |
| [base] Revision 255442 | svnweb.freebsd.org, text/html | CONFIRM svnweb.freebsd.org/base?view=revision&revision=255442 |

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 | 9.2 | rc1 | All | All |
| Operating System | Freebsd | Freebsd | 9.2 | rc2 | All | All |
| Operating System | Freebsd | Freebsd | 9.2 | rc1 | All | All |
| Operating System | Freebsd | Freebsd | 9.2 | rc2 | All | All |

cpe:2.3:o:freebsd:freebsd:9.2:rc1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:9.2:rc2:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:9.2:rc1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:9.2:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→