



# CVE-2017-15037

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-15037                                                                                                           |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2017-10-05 07:29:00 UTC                                                                                                  |
| <b>Updated</b>         | 2017-10-13 19:58:00 UTC                                                                                                  |
| <b>Description</b>     | In FreeBSD through 11.1, the smb_strdupin function in sys/netmb/smb_subr.c has a race condition with a resultant out-of- |

## Risk And Classification

**Problem Types:** CWE-362 | CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor  | Product | Version | Update | Edition | Language |
|------------------|---------|---------|---------|--------|---------|----------|
| Operating System | Freebsd | Freebsd | All     | All    | All     | All      |

## References

| Reference                                                                     | Source  | Link                                                             | Tags                  |
|-------------------------------------------------------------------------------|---------|------------------------------------------------------------------|-----------------------|
| FreeBSD 'sys/netmb/smb_subr.c' Local Race Condition Vulnerability             | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a> | Third Party Advisory, |
| 222687 – smb_strdupin() does not properly check the length of string duped-in | CONFIRM | <a href="http://bugs.freebsd.org">bugs.freebsd.org</a>           | Issue Tracking, Vend  |
| [base] Revision 324102                                                        | CONFIRM | <a href="http://svnweb.freebsd.org">svnweb.freebsd.org</a>       | Issue Tracking, Vend  |
| CVE Program record                                                            | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                     | canonical             |
| NVD vulnerability detail                                                      | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis   |

No vendor comments have been submitted for this CVE.

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)