



CVE-2015-3332

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-3332
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-27 10:59:00 UTC
Updated	2016-04-11 18:54:00 UTC
Description	A certain backport in the TCP Fast Open implementation for the Linux kernel before 3.18 does not properly maintain a cour

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	L
Bug 1213951 – CVE-2015-3332 kernel: TCP Fast Open local DoS	CONFIRM	b
Debian -- Security Information -- DSA-3237-1 linux	DEBIAN	v
article.gmane.org 522: Connection timed out	MLIST	a
oss-security - TCP Fast Open local DoS in some Linux stable branches	MLIST	v
#782515 - [regression] BUG in process context when using TCP Fast Open (CVE-2015-2015-3332) - Debian Bug report logs	CONFIRM	b
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

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](#)