



CVE-2016-1583

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

Summary

CVE	CVE-2016-1583
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-27 10:59:00 UTC
Updated	2023-09-12 14:55:00 UTC
Description	The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain priv

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All

Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All

References

Reference

USN-3008-1: Linux kernel (Qualcomm Snapdragon) vulnerability | Ubuntu

[security-announce] SUSE-SU-2016:2009-1: important: Security update for

ecryptfs: forbid opening files without mmap handler · torvalds/linux@2f36db7 · GitHub

[security-announce] SUSE-SU-2016:1961-1: important: Security update for

USN-3005-1: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2016:193/-1: important: Security update for
[security-announce] SUSE-SU-2016:2010-1: important: Security update for
[security-announce] SUSE-SU-2016:2005-1: important: Security update for
[security-announce] SUSE-SU-2016:2002-1: important: Security update for
USN-2999-1: Linux kernel vulnerability Ubuntu
[security-announce] openSUSE-SU-2016:1641-1: important: Security update
oss-security - [vs-plain] Linux kernel stack overflow via ecryptfs and /proc/\$pid/environ
USN-3000-1: Linux kernel (Utopic HWE) vulnerabilities Ubuntu
836 - Linux: Stack overflow via ecryptfs and /proc/\$pid/environ - project-zero - Monorail
Red Hat Customer Portal
Bug 1344721 – CVE-2016-1583 kernel: Stack overflow via ecryptfs and /proc/\$pid/environ
[security-announce] SUSE-SU-2016:2007-1: important: Security update for
[security-announce] SUSE-SU-2016:1985-1: important: Security update for
kernel/git/torvalds/linux.git - Linux kernel source tree
Merge branch 'stacking-fixes' (vfs stacking fixes from Jann) · torvalds/linux@f5364c1 · GitHub
Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive
USN-2998-1: Linux kernel (Trusty HWE) vulnerabilities Ubuntu
[security-announce] SUSE-SU-2016:1994-1: important: Security update for
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities Ubuntu
Red Hat Customer Portal
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities Ubuntu
[security-announce] SUSE-SU-2016:1995-1: important: Security update for
[security-announce] SUSE-SU-2016:2014-1: important: Security update for
USN-3007-1: Linux kernel (Raspberry Pi 2) vulnerabilities Ubuntu
kernel/git/torvalds/linux.git - Linux kernel source tree
[security-announce] SUSE-SU-2016:1672-1: important: Security update for
USN-3002-1: Linux kernel (Wily HWE) vulnerabilities Ubuntu
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.6.3
[security-announce] SUSE-SU-2016:2006-1: important: Security update for
Red Hat Customer Portal
Debian -- Security Information -- DSA-3607-1 linux
[security-announce] SUSE-SU-2016:1596-1: important: Security update for
USN-2996-1: Linux kernel vulnerabilities Ubuntu
Linux Kernel - 'ecryptfs' '/proc/\$pid/environ' Local Privilege Escalation - Linux local Exploit
ecryptfs: don't allow mmap when the lower fs doesn't support it · torvalds/linux@f0fe970 · GitHub
oss-security - Re: [vs-plain] Linux kernel stack overflow via ecryptfs and /proc/\$pid/environ

USN-3003-1: Linux kernel vulnerabilities | Ubuntu

USN-3006-1: Linux kernel vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2016:2105-1: important: Security update for

[security-announce] SUSE-SU-2016:1696-1: important: Security update for

[security-announce] openSUSE-SU-2016:2184-1: important: Security update

Linux ecryptfs Stack Overflow ~ Packet Storm

[security-announce] SUSE-SU-2016:2000-1: important: Security update for

USN-2997-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu

Linux Kernel CVE-2016-1583 Stack-Based Buffer Overflow Vulnerability

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[671047](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

© [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](#)