



CVE-2015-1805

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

Summary

CVE	CVE-2015-1805
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-08 10:59:00 UTC
Updated	2018-01-05 02:30:00 UTC
Description	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider th

Risk And Classification

Problem Types: CWE-17

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
[security-announce] SUSE-SU-2015:1489-1: important: Live patch for the L	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2015:1491-1: important: Live patch for the L	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2015:1487-1: important: Live patch for the L	SUSE	lists.opensuse.org

Linux Kernel I/O Vector Memory Corruption Flaw Lets Local Users Gain Root Privileges - SecurityTracker	SECTrack	www.securitytracker.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
USN-2967-2: Linux kernel (OMAP4) vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Bug 1202855 – CVE-2015-1805 kernel: pipe: iovec overrun leading to memory corruption	CONFIRM	bugzilla.redhat.com
[security-announce] SUSE-SU-2015:1224-1: important: Security update for	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Nexus Security Bulletin—April 2016 Android Open Source Project	CONFIRM	source.android.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
RHSA-2015:1190	REDHAT	rhn.redhat.com
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	SUSE	lists.opensuse.org
Linux Kernel 'fs/pipe.c' Multiple Local Memory Corruption Vulnerabilities	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Android Security Bulletin—May 2016 Android Open Source Project	CONFIRM	source.android.com
[security-announce] SUSE-SU-2015:1611-1: important: Security update for	SUSE	lists.opensuse.org
USN-2680-1: Linux kernel (Trusty HWE) vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com
oss-security - CVE-2015-1805 Linux kernel: pipe: iovec overrun leading to memory corruption	MLIST	www.openwall.com
new helper: copy_page_from_iter() · torvalds/linux@f0d1bec · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
switch pipe_read() to copy_page_to_iter() · torvalds/linux@637b58c · GitHub	CONFIRM	github.com
USN-2679-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
USN-2681-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
[security-announce] SUSE-SU-2015:1592-1: important: Security update for	SUSE	lists.opensuse.org
USN-2967-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
[security-announce] SUSE-SU-2015:1324-1: important: Security update for	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
[security-announce] SUSE-SU-2015:1490-1: important: Live patch for the L	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2015:1488-1: important: Live patch for the L	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-3290-1 linux	DEBIAN	www.debian.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

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