



CVE-2016-0728

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

Summary

CVE	CVE-2016-0728
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-08 03:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object refere

Risk And Classification

Problem Types: NVD-CWE-Other

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All

Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	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	6.0.1	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	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	6.0.1	All	All	All
Application	Hp	Server Migration Pack	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	MISC	acc
Use after free vulnerability in Linux kernel keychain management (CVE-2016-0728) - Red Hat Customer Portal	MISC	acc
USN-2870-2: Linux kernel (Trusty HWE) vulnerability Ubuntu	UBUNTU	ww
USN-2873-1: Linux kernel (Utopic HWE) vulnerability Ubuntu	UBUNTU	ww
Red Hat Customer Portal	MISC	acc
[SECURITY] Fedora 23 Update: kernel-4.3.3-303.fc23	FEDORA	list
[security-announce] SUSE-SU-2016:0757-1: important: Security update for	SUSE	list
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.1	CONFIRM	ww
Linux Kernel 4.4.1 - REFCOUNT Overflow/Use-After-Free in Keyrings Privilege Escalation (1)	EXPLOIT-DB	ww
Nexus Security Bulletin - March 2016 Android Open Source Project	CONFIRM	sou
USN-2871-2: Linux kernel (Vivid HWE) vulnerability Ubuntu	UBUNTU	ww
USN-2872-1: Linux kernel vulnerability Ubuntu	UBUNTU	ww
Debian -- Security Information -- DSA-3448-1 linux	DEBIAN	ww
Red Hat Customer Portal	REDHAT	rhn
[security-announce] SUSE-SU-2016:0747-1: important: Security update for	SUSE	list
[security-announce] SUSE-SU-2016:0752-1: important: Security update for	SUSE	list
[security-announce] SUSE-SU-2016:0750-1: important: Security update for	SUSE	list
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.
USN-2872-3: Linux kernel (Raspberry Pi 2) vulnerability Ubuntu	UBUNTU	ww
Red Hat Customer Portal	REDHAT	rhn
KEYS: Fix keyring ref leak in join_session_keyring() · torvalds/linux@23567fd · GitHub	CONFIRM	gitf
[security-announce] SUSE-SU-2016:0755-1: important: Security update for	SUSE	list
[security-announce] SUSE-SU-2016:0751-1: important: Security update for	SUSE	list
[security-announce] SUSE-SU-2016:0753-1: important: Security update for	SUSE	list
Analysis and Exploitation of a Linux Kernel Vulnerability (CVE-2016-0728) Perception Point	MISC	per
Document Display HPE Support Center	CONFIRM	h20
[security-announce] SUSE-SU-2016:0205-1: important: Security update for	SUSE	list
Red Hat Customer Portal	REDHAT	rhn
USN-2871-1: Linux kernel vulnerability Ubuntu	UBUNTU	ww

Oracle Linux Bulletin - January 2016	CONFIRM	ww
USN-2872-2: Linux kernel (Wily HWE) vulnerability Ubuntu	UBUNTU	ww
Red Hat Customer Portal	MISC	acc
[security-announce] SUSE-SU-2016:0746-1: important: Security update for	SUSE	list:
Linux Kernel Session Keyring Reference Count Overflow Bug Lets Local Users Obtain Root Privileges - SecurityTracker	SECTRACK	ww
oss-security - Linux kernel: use after free in keyring facility.	MLIST	ww
[SECURITY] Fedora 22 Update: kernel-4.3.4-200.fc22	FEDORA	list:
CVE-2016-0728 - Red Hat Customer Portal	MISC	acc
CVE-2016-0728 Linux Kernel Privilege Escalation Vulnerability in NetApp Products NetApp Product Security	CONFIRM	sec
SA112 : Linux Kernel Keyring Privilege Escalation Symantec	CONFIRM	bto
[security-announce] SUSE-SU-2016:0756-1: important: Security update for	SUSE	list:
Document Display HPE Support Center	CONFIRM	h20
Bug 1297475 – CVE-2016-0728 kernel: Possible use-after-free vulnerability in keyring facility	CONFIRM	buq
[security-announce] SUSE-SU-2016:0745-1: important: Security update for	SUSE	list:
USN-2870-1: Linux kernel vulnerability Ubuntu	UBUNTU	ww
Red Hat Customer Portal	MISC	acc
HPSBHF03436	HP	h20
[security-announce] SUSE-SU-2016:0341-1: important: Security update for	SUSE	list:
Linux Kernel CVE-2016-0728 Local Privilege Escalation Vulnerability	BID	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

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](#).

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