



CVE-2014-0196

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

Summary

CVE	CVE-2014-0196
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-07 10:55:00 UTC
Updated	2023-02-13 00:36:00 UTC
Description	The n_tty_write function in drivers/tty/n_tty.c in the Linux kernel through 3.14.3 does not properly manage tty driver access

Risk And Classification

EPSS: 0.485560000 probability, percentile 0.977340000 (date 2026-04-02)

CISA KEV: Listed on 2023-05-12; due 2023-06-02; ransomware use Unknown

Problem Types: CWE-362

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Race Condition Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://lkml.iu.edu/hypermail/linux/kernel/1609.1/02103.html ; https://nvd.nist.gov/vuln/detail/CVE-2014-0196

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Protocol Security Module	All	All	All	All
Application	F5	Big-ip Wan Optimization Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-iq Application Delivery Controller	4.5.0	All	All	All
Application	F5	Big-iq Application Delivery Controller	4.5.0	All	All	All
Application	F5	Big-iq Centralized Management	4.6.0	All	All	All
Application	F5	Big-iq Centralized Management	4.6.0	All	All	All
Application	F5	Big-iq Cloud	All	All	All	All
Application	F5	Big-iq Cloud And Orchestration	1.0.0	All	All	All
Application	F5	Big-iq Cloud And Orchestration	1.0.0	All	All	All
Application	F5	Big-iq Device	All	All	All	All
Application	F5	Big-iq Security	All	All	All	All
Application	F5	Enterprise Manager	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise High Availability Extension	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise High Availability Extension	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All

References

Reference	Source
[security-announce] SUSE-SU-2014:0667-1: important: Security update for	SUSE
Debian -- Security Information -- DSA-2928-1 linux-2.6	DEBIAN
n_tty: Fix n_tty_write crash when echoing in raw mode · torvalds/linux@4291086 · GitHub	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC
USN-2196-1: Linux kernel vulnerability Ubuntu	UBUNTU
USN-2203-1: Linux kernel vulnerability Ubuntu	UBUNTU
pastebin.com/raw.php	MISC
Linux kernel 3.14-rc1 <= 3.15-rc4 - Raw Mode PTY Local Echo Race Condition (x64) Local Privilege Escalation	EXPLOIT-
USN-2202-1: Linux kernel vulnerability Ubuntu	UBUNTU
USN-2197-1: Linux kernel (EC2) vulnerability Ubuntu	UBUNTU
Security Advisory SA59599 - Ubuntu update for kernel - Secunia	SECUNIA
USN-2201-1: Linux kernel (Saucy HWE) vulnerability Ubuntu	UBUNTU
oss-security - CVE-2014-0196: Linux kernel pty layer race condition memory corruption	MLIST
Android Security Bulletin—July 2016 Android Open Source Project	CONFIRM
USN-2204-1: Linux kernel vulnerability Ubuntu	UBUNTU
[security-announce] SUSE-SU-2014:0683-1: important: Security update for	SUSE
USN-2199-1: Linux kernel (Quantal HWE) vulnerability Ubuntu	UBUNTU
Red Hat Customer Portal	REDHAT
Bug 875690 – VUL-0: CVE-2014-0196: kernel: memory corruption via a race in pty write handling	CONFIRM

Security Advisory SA59218 - F5 Multiple Products Linux Kernel "n_tty_write()" Race Condition Vulnerability - Secunia	SECUNIA
Bug 1094232 – CVE-2014-0196 kernel: pty layer race condition leading to memory corruption	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
Security Advisory SA59262 - Oracle Linux update for kernel - Secunia	SECUNIA
USN-2200-1: Linux kernel (Raring HWE) vulnerability Ubuntu	UBUNTU
USN-2198-1: Linux kernel vulnerability Ubuntu	UBUNTU
support.f5.com/kb/en-us/solutions/public/15000/300/sol15319.html	CONFIRM
106646	OSVDB
Debian -- Security Information -- DSA-2926-1 linux	DEBIAN
linux.oracle.com ELSA-2014-0771 - kernel security and bug fix update	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

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](#)