



CVE-2017-2636

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

Summary

CVE	CVE-2017-2636
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-07 22:59:00 UTC
Updated	2023-02-24 18:43:00 UTC
Description	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a deni

Risk And Classification

Problem Types: CWE-362 | CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

References

Reference	Source
Linux Kernel Race Condition in N_HLDC Driver Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack
CVE-2017-2636 - Red Hat Customer Portal	MISC
Bug 1428319 – CVE-2017-2636 kernel: Race condition access to n_hdlc.tbuf causes double free in n_hdlc_release()	CONFIRM
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Debian -- Security Information -- DSA-3804-1 linux	DEBIAN
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Local kernel privilege escalation in the HDLC TTY line discipline implementation - CVE-2017-2636 - Red Hat Customer Portal	MISC

oss-security - Linux kernel: CVE-2017-2636: local privilege escalation flaw in n_hdlc	MLIST
Red Hat Customer Portal	REDHAT
Linux Kernel CVE-2017-2636 Local Privilege Escalation Vulnerability	BID
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
CVE-2017-2636: exploit the race condition in the n_hdlc Linux kernel driver bypassing SMEP	MISC
Red Hat Customer Portal	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378155](#) Virtuozzo Linux Security Update for perf (VZLSA-2017:0892)

[378168](#) Virtuozzo Linux Security Update for perf (VZLSA-2017:0933)

© [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