CVE-2016-3951

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-3951
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-02 10:59:00 UTC
Updated	2017-08-13 01:29:00 UTC
Description	Double free vulnerability in drivers/net/usb/cdc_ncm.c in the Linux kernel before 4.5 allows physically proximate attackers to

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	15.10	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	Linux	Linux Kernel	4.5.0	rc7	All	All
Operating System	Linux	Linux Kernel	4.5.0	rc7	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12	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 Real Time Extension	12	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Real Time Extension	12	sp1	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	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	12.0	sp1	All	All
Application	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
Application	Suse	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	12.0	All	All	All

References

Reference
[security-announce] openSUSE-SU-2016:1382-1: important: Security update
kernel/git/torvalds/linux.git - Linux kernel source tree
1324782 – (CVE-2016-3951) CVE-2016-3951 kernel: crash on invalid USB device descriptors (usbnet driver)
USN-3000-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu
Linux Kernel CVE-2016-3951 Null Pointer Deference Local Denial of Service Vulnerability
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
USN-3021-2: Linux kernel (OMAP4) vulnerabilities | Ubuntu
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu
kernel/git/torvalds/linux.git - Linux kernel source tree
USN-3021-1: Linux kernel vulnerabilities | Ubuntu
USN-3002-1: Linux kernel (Wily HWE) vulnerabilities | Ubuntu
usbnet: cleanup after bind() in probe() · torvalds/linux@1666984 · GitHub
Debian -- Security Information -- DSA-3607-1 linux
[security-announce] SUSE-SU-2016:1764-1: important: Security update for
USN-2989-1: Linux kernel vulnerabilities | Ubuntu
USN-3003-1: Linux kernel vulnerabilities | Ubuntu
Re: Possible double-free in the usbnet driver — Linux Network Development

[security-announce] SUSE-SU-2016:1690-1: important: Security update for
[security-announce] SUSE-SU-2016:1696-1: important: Security update for
oss-security - Fwd: CVE Request: Linux: usbnet: memory corruption triggered by invalid USB descriptor
cdc_ncm: do not call usbnet_link_change from cdc_ncm_bind · torvalds/linux@4d06dd5 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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