



CVE-2016-2185

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

Summary

CVE	CVE-2016-2185
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-02 10:59:00 UTC
Updated	2023-09-12 14:55:00 UTC
Description	The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proxir

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	12.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	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	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Server	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	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	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	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	11.0	sp4	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	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

References

Reference

[security-announce] [openSUSE-SU-2016:1382-1](#): important: Security update

Input: ati_remote2 - fix crashes on detecting device with invalid des... · torvalds/linux@950336b · GitHub

USN-2969-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu

[security-announce] [SUSE-SU-2016:1707-1](#): important: Security update for

USN-2971-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu

USN-2968-1: Linux kernel vulnerabilities | Ubuntu

[kernel/git/torvalds/linux.git](#) - Linux kernel source tree

20160315 Re: [oss-2016-18](#): Multiple Local RedHat Enterprise Linux DoS - RHEL 7.1 Kernel crashes on invalid USB device descriptors (ati_re

1283363 – [CVE-2016-2185](#) Local RedHat Enterprise Linux DoS – RHEL 7.1 Kernel crashes on invalid USB device descriptors (ati_remote2 d

[security-announce] [SUSE-SU-2016:2074-1](#): important: Security update for

[security-announce] [SUSE-SU-2016:1672-1](#): important: Security update for

USN-2970-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu

USN-2970-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu

1283362 – CVE-2016-2185 Local RedHat Enterprise Linux DoS – RHEL 7.1 Kernel crashes on invalid USB device descriptors (ati_remote2 d

USN-2968-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu

Bugtraq: oss-2016-18: Multiple Local RedHat Enterprise Linux DoS – RHEL 7.1 Kernel crashes on invalid USB device descriptors (ati_remote

Debian -- Security Information -- DSA-3607-1 linux

USN-2996-1: Linux kernel vulnerabilities | Ubuntu

Linux Kernel CVE-2016-2185 Null Pointer Deference Local Denial of Service Vulnerability

USN-2971-1: Linux kernel vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2016:1764-1: important: Security update for

[security-announce] SUSE-SU-2016:1690-1: important: Security update for

[security-announce] SUSE-SU-2016:1696-1: important: Security update for

1317014 – (CVE-2016-2185) CVE-2016-2185 kernel: Kernel panic on invalid USB device descriptor (ati_remote2 driver)

www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.1

USN-2997-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu

USN-2971-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

671064 EulerOS Security Update for kernel (EulerOS-SA-2019-2599)

© 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](#)