CVE-2010-4242

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-4242
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-11 03:00:00 UTC
Updated	2018-10-10 20:07:00 UTC
Description	The hci_uart_tty_open function in the HCI UART driver (drivers/bluetooth/hci_ldisc.c) in the Linux kernel 2.6.36, and possib

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.36	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	All	All	All

References

Reference	Source	Link
SUSE update for kernel - Advisories - Community	SECUNIA	secu
CVE-2010-4242: Linux kernel Bluetooth HCI UART Invalid Pointer Access « xorl %eax, %eax	MISC	xorl.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
Support	REDHAT	www
SecurityFocus	BUGTRAQ	www
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.k
VMSA-2011-0012.2	CONFIRM	www
Red Hat update for kernel - Advisories - Community	SECUNIA	secu
Linux Kernel 'hci_uart_tty_open()' Local Denial of Service Vulnerability	BID	www
Support	REDHAT	www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
Red Hat update for kernel - Secunia.com	SECUNIA	secu

About Secunia Research | Flexera	SECUNIA	secu
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
Red Hat update for kernel - Secunia.com	SECUNIA	secu
LKML: Alan Cox: Peculiar stuff in hci_ath3k/badness in hci_uart	MLIST	lkml
IBM X-Force Exchange	XF	exch
access.redhat.com	REDHAT	www
641410 – (CVE-2010-4242) CVE-2010-4242 kernel: missing tty ops write function presence check in hci_uart_tty_open()	CONFIRM	bug:
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

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 registred 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**