CVE-2010-4251

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

Summary

CVE	CVE-2010-4251
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-26 16:55:00 UTC
Updated	2023-02-13 04:28:00 UTC
Description	The socket implementation in net/core/sock.c in the Linux kernel before 2.6.34 does not properly manage a backlog of rece

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All

References

Reference	Source	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kerne
[PATCH 1/8] net: add limit for socket backlog | KernelTrap	MLIST	kerneltra
657303 – (CVE-2010-4251, CVE-2010-4805) CVE-2010-4251 CVE-2010-4805 kernel: unlimited socket backlog DoS	CONFIRM	bugzilla.r
SecurityFocus	BUGTRAQ	www.sec
VMSA-2011-0012.2	CONFIRM	www.vm
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kerne

About Secunia Research | Flexera	SECUNIA	secunia.c
Linux Kernel Unix Socket Backlog Local Denial of Service Vulnerability	BID	www.sec
404: File not found	CONFIRM	www.ker
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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**