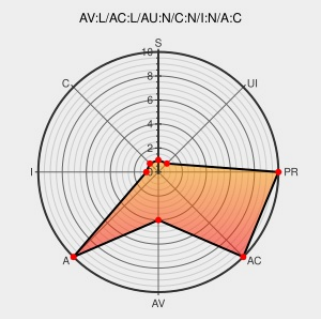
CVE-2011-1083

Published on: 04/02/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:22 AM UTC

CVE-2011-1083

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The epoll implementation in the Linux kernel 2.6.37.2 and earlier does not properly traverse a tree of epoll file descriptors, which allows local users to cause a denial of service (CPU consumption) via a crafted application that makes epoll_create and epoll_ctl system calls.

CVE-2011-1083 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
article.gmane.org | 522: Connection timed out	Broken Link, article.gmane.org, text/html, Inactive Link, Not Archived	MLIST [linux-kernel] 20110225 [PATCH] optimize epoll loop detection
article.gmane.org | 522: Connection timed out	Broken Link, article.gmane.org, text/html, Inactive Link, Not Archived	MLIST [linux-kernel] 20110228 Re: [PATCH] optimize epoll loop detection
[security-announce] SUSE-SU-2012:0554-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SU-2012:0554
Linux Kernel epoll Denial of Service Vulnerability - Secunia.com	Third Party Advisory, web.archive.org	SECUNIA 43522

	text/html	
oss-security - CVE request: kernel: Multiple DoS issues in epoll	Mailing List Patch Third Party Advisory openwall.com text/html	MLIST [oss-security] 20110301 CVE request: kernel: Multiple DoS issues in epoll
No Description Provided	Broken Link www.osvdb.org Inactive Link Not Archived	OSVDB 71265
Bug 681578 – CVE-2011-1083 kernel: excessive in kernel CPU consumption when creating large nested epoll structures	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=681578
Security Advisory SA48115 - Red Hat update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 48115
oss-security - Re: CVE request: kernel: Multiple DoS issues in epoll	Mailing List Patch openwall.com text/html	MLIST [oss-security] 20110302 Re: CVE request: kernel: Multiple DoS issues in epoll
access.redhat.com	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:0862
About Secunia Research | Flexera	Third Party Advisory secunia.com Depreciated Link text/plain	SECUNIA 48964
article.gmane.org | 522: Connection timed out	Broken Link article.gmane.org text/html Inactive Link Not Archived	MLIST [linux-kernel] 20110226 Re: [PATCH] optimize epoll loop detection
[security-announce] SUSE-SU-2012:0616-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2012:0616
Security Advisory SA48410 - OpenVZ update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 48410
Security Advisory SA48898 - SUSE update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 48898

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:-:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:-:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:-:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:-:*:*

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→