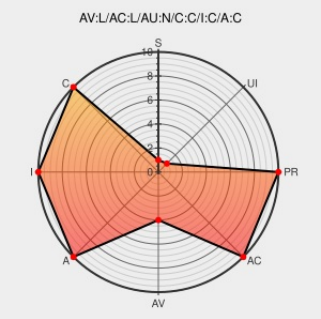
CVE-2010-2240

Published on: 09/03/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:21:00 AM UTC

CVE-2010-2240

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



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

The do_anonymous_page function in mm/memory.c in the Linux kernel before 2.6.27.52, 2.6.32.x before 2.6.32.19, 2.6.34.x before 2.6.34.4, and 2.6.35.x before 2.6.35.2 does not properly separate the stack and the heap, which allows context-dependent attackers to execute arbitrary code by writing to the bottom page of a shared memory segment, as demonstrated by a memory-exhaustion attack against the X.Org X server.

CVE-2010-2240 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Support	www.redhat.com text/html	REDHAT RHSA-2010:0670
Support / Security / Advisories / / MDVSA-2010:172 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2010:172
Support	www.redhat.com text/html	REDHAT RHSA-2010:0882
VMSA-2011-0007	www.vmware.com text/html	CONFIRM www.vmware.com/security/advisories/VMSA-2011-0007.html
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=320b2b8de12698082609ebbc1a17165727f4c893

	Inactive Link Not Archived	
	Exploit www.invisiblethingslab.com application/pdf	MISC www.invisiblethingslab.com/resources/misc-2010/xorg-large-memory-attacks.pdf
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20110428 VMSA-2011-0007 VMware ESXi and ESX Denial of Service and third party updates for Likewise components and ESX Service Console
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0631
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0661
Bug 606611 – CVE-2010-2240 kernel: mm: keep a guard page below a grow-down stack segment	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=606611
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27.52
access.redhat.com | CVE-2010-2240	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2010-2240
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.32.19
SecurityTracker.com Archives - Linux Kernel Stack Memory Management Lets Local Users Gain Root Privileges	securitytracker.com text/html	SECTRACK 1024344
[Security-announce] VMSA-2011-0007 VMware ESXi and ESX Denial of Service and third party updates for Likewise components and ESX Service Console	lists.vmware.com text/html	MLIST [security-announce] 20110428 VMSA-2011-0007 VMware ESXi and ESX Denial of Service and third party updates for Likewise components and ESX Service Console
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0660
Support / Security / Advisories / / MDVSA-2010:198 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2010:198
Support	www.redhat.com text/html	REDHAT RHSA-2010:0660
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:13247
VMSA-2011-0009.3	www.vmware.com text/html	CONFIRM www.vmware.com/security/advisories/VMSA-2011-0009.html
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0677
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0676
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0882

mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2011:051
Debian -- Security Information -- DSA-2094-1 linux-2.6	www.debian.org Depreciated Link text/html	DEBIAN DSA-2094
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.35.2
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2010:0661
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.34.4
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2010:0670

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	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.18	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.32.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.35.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.17	All	All	All
Operating	Linux	Linux Kernel	2.6.32.18	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.32.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.34.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.35.1	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.32:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.11:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.12:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.13:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.14:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.15:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.16:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.17:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.9:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.35.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.11:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.12:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.13:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.14:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.15:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.16:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.17:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32.9:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.34.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.35.1:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→