CVE-2009-2691

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

Summary

CVE	CVE-2009-2691
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-14 15:16:27 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The mm_for_maps function in fs/proc/base.c in the Linux kernel 2.6.30.4 and earlier allows local users to read (1) maps and

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.30	All	All	All

Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc7-git6	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
LKML: Oleg Nesterov: [PATCH 0/1] mm_for_maps: simplify, use ptrace_may_access()	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
Debian -- Security Information -- DSA-2005-1 linux-2.6.24	af854a3a-2127-422b-9
[SECURITY] Fedora 11 Update: kernel-2.6.29.6-217.2.16.fc11	af854a3a-2127-422b-9
Linux Kernel "mm_for_maps()" Information Disclosure - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-9
Fedora update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-9
504 Gateway Time-out	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-9
oss-security - CVE-2009-2691 kernel: /proc/$pid/maps visible during initial setuid ELF loading	af854a3a-2127-422b-9
516171 – (CVE-2009-2691) CVE-2009-2691 kernel: /proc/$pid/maps visible during initial setuid ELF loading	af854a3a-2127-422b-9
'[PATCH 1/2] mm_for_maps: shift down_read(mmap_sem) to the caller' - MARC	af854a3a-2127-422b-9
LKML: Oleg Nesterov: [PATCH 1/1] mm_for_maps: simplify, use ptrace_may_access()	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-9
Red Hat Customer Portal	af854a3a-2127-422b-9
Webmail - OVH	af854a3a-2127-422b-9
'[PATCH 2/2] mm_for_maps: take ->cred_guard_mutex to fix the race' - MARC	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE ORG

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-11-04	Mark J Cox	The Red Hat Security Response Team has rated this issue as having moderate security impact.

There are currently no legacy QID mappings associated with this CVE.