CVE-2009-2768

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

Summary

CVE	CVE-2009-2768
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 load_flat_shared_library function in fs/binfmt_flat.c in the flat subsystem in the Linux kernel before 2.6.31-rc6 allows loc

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-476 | CWE-824 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

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	2.6.31	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc5	All	All

Vendor Declared Affected Products

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

References

Reference	Source
oss-security - CVE request: kernel: flat: fix uninitialized ptr with shared libs	af854a3a-2127-422b-91ae-364da266110
thread.gmane.org | 522: Connection timed out	af854a3a-2127-422b-91ae-364da266110
404: File not found	af854a3a-2127-422b-91ae-364da266110
Linux Kernel Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91ae-364da266110
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da266110

git.kernel.org	af854a3a-2127-422b-91ae-364da26611(
404: File not found	af854a3a-2127-422b-91ae-364da26611(
LKML: Bernd Schmidt: Fix for shared flat binary format in 2.6.30	af854a3a-2127-422b-91ae-364da26611(
mandriva.com	af854a3a-2127-422b-91ae-364da26611(
Linux Kernel 'binfmt_flat.c' NULL Pointer Dereference Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da26611(
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-08-18	Mark J Cox	Not vulnerable. This issue did not affect the versions of Linux kernel as shipped with Red Hat En

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