CVE-2011-1776

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

Summary

CVE	CVE-2011-1776
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-06 16:55:07 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The is_gpt_valid function in fs/partitions/efi.c in the Linux kernel before 2.6.39 does not check the size of an Extensible Firm

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
2.0	nvd@nist.gov	Primary	5.6		AV:L/AC:L/Au:N/C:P/I:N/A:C

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:P/I:N/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	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
404: File not found	af854a3a-2127-422b-91ae-364da2661108	www.kern
access.redhat.com	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat
oss-security - Re: CVE request: kernel: validate size of EFI GUID partition entries	af854a3a-2127-422b-91ae-364da2661108	openwall.c
git.kernel.org	af854a3a-2127-422b-91ae-364da2661108	git.kernel.c
www.pre-cert.de/advisories/PRE-SA-2011-04.txt	af854a3a-2127-422b-91ae-364da2661108	www.pre-c

linux kernel 2.6.38.8 information disclosure, denial-of-service - SecurityReason.com	af854a3a-2127-422b-91ae-364da2661108	securityrea
Linux Kernel EFI Partition Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secu
Bug 703026 – CVE-2011-1776 kernel: validate size of EFI GUID partition entries	af854a3a-2127-422b-91ae-364da2661108	bugzilla.re
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE	git.kernel.(
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.