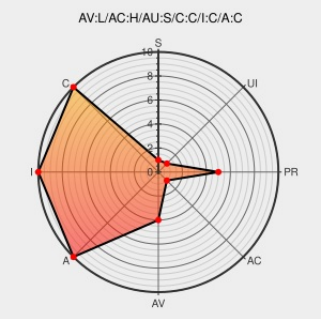
CVE-2013-2851

Published on: 06/07/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2851

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



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

Format string vulnerability in the register_disk function in block/genhd.c in the Linux kernel through 3.9.4 allows local users to gain privileges by leveraging root access and writing format string specifiers to /sys/module/md_mod/parameters/new_array in order to create a crafted /dev/md device name.

CVE-2013-2851 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
USN-1941-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1941-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1645
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0284
oss-security - Linux kernel format string flaws	www.openwall.com text/html	MLIST [oss-security] 20130606 Linux kernel format string flaws
[security-announce] SUSE-SU-2013:1473-1:	lists.opensuse.org	SUSE SUSE-SU-2013:1473

important: Security update for	text/html	
USN-1913-1: Linux kernel (EC2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1913-1
Bug 969515 – CVE-2013-2851 kernel: block: passing disk names as format strings	Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=969515
USN-1942-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1942-1
USN-1912-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1912-1
[security-announce] SUSE-SU-2013:1474-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2013:1474
openSUSE-SU-2013:1971-1: moderate: kernel: security and bugfix update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1971
Debian -- Security Information -- DSA-2766-1 linux-2.6	www.debian.org Depreciated Link text/html	DEBIAN DSA-2766
'[PATCH 1/8] block: do not pass disk names as format strings' - MARC	marc.info text/x-diff	MLIST [linux-kernel] 20130606 [PATCH 1/8] block: do not pass disk names as format strings
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1783

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	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All
Operating System	Linux	Linux Kernel	3.9	rc6	All	All
Operating System	Linux	Linux Kernel	3.9	rc7	All	All
Operating	Linux	Linux Kernel	3.9.0	All	All	All

System						
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All
Operating System	Linux	Linux Kernel	3.9	rc6	All	All
Operating System	Linux	Linux Kernel	3.9	rc7	All	All
Operating System	Linux	Linux Kernel	3.9.0	All	All	All
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.9:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→