



CVE-2013-2852

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

Last Modified on: 08/11/2023 06:14:00 PM UTC

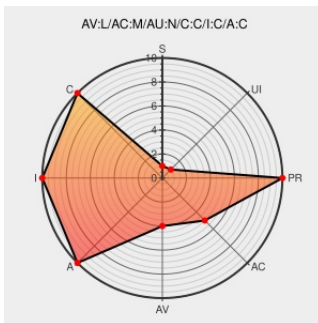
CVE-2013-2852

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Format string vulnerability in the b43_request_firmware function in drivers/net/wireless/b43/main.c in the Broadcom B43 wireless driver in the Linux kernel through 3.9.4 allows local users to gain privileges by leveraging root access and including format string specifiers in an fwpostfix modprobe parameter, leading to improper construction of an

error message.

CVE-2013-2852 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

USN-1919-1: Linux kernel vulnerability |
Ubuntu

[www.ubuntu.com](http://www.ubuntu.com/text/html)
[text/html](#)

[UBUNTU USN-1919-1](#)

Red Hat Customer Portal

[web.archive.org](http://web.archive.org/text/html)
[text/html](#)
Inactive Link Not Archived

[REDHAT RHSA-2013:1051](#)

USN-1914-1: Linux kernel vulnerability |
Ubuntu

[www.ubuntu.com](http://www.ubuntu.com/text/html)
[text/html](#)

[UBUNTU USN-1914-1](#)

USN-1918-1: Linux kernel (OMAP4)
vulnerability | Ubuntu

[www.ubuntu.com](http://www.ubuntu.com/text/html)
[text/html](#)

[UBUNTU USN-1918-1](#)

oss-security - Linux kernel format string flaws

www.openwall.com

[MLIST \[oss-security\] 20130606 Linux kernel format string](#)

	text/html	flaws
[security-announce] SUSE-SU-2013:1473-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2013:1473
USN-1915-1: Linux kernel (Quantal HWE) vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1915-1
Bug 969518 – CVE-2013-2852 kernel: b43: format string leaking into error msgs	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=969518
USN-1920-1: Linux kernel (OMAP4) vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1920-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1450
USN-1900-1: Linux kernel (EC2) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1900-1
USN-1930-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1930-1
kernel/git/linville/wireless.git - Wireless tree for feeding the net tree.	Exploit Patch git.kernel.org text/html	 CONFIRM git.kernel.org/cgit/linux/kernel/git/linville/wireless.git/commit/?id=9538cbaab6e8b8046039b4b2eb6c9d614dc782bd
USN-1916-1: Linux kernel (Raring HWE) vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1916-1
USN-1899-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1899-1
USN-1917-1: Linux kernel vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1917-1
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 Deprecated Link text/html	 DEBIAN DSA-2766
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All

Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Linux	Linux Kernel	All	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	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:canonical:ubuntu_linux:10.04.*.*.*:-.*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04.*.*.*:-.*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10.*.*.*.*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:13.04.*.*.*.*.*.*:						
cpe:2.3:o:debian:debian_linux:6.0.*.*.*.*.*.*:						
cpe:2.3:o:linux:linux_kernel:*.*.*.*.*.*.*:						
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:3.9.0.*.*.*.*.*:
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→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report