

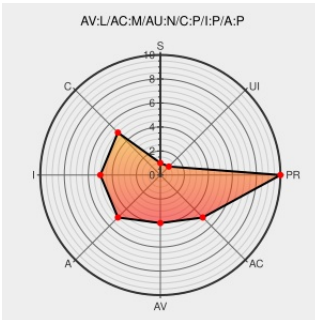


CVE-2013-1929

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

Last Modified on: 02/13/2023 04:42:00 AM UTC

CVE-2013-1929

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Heap-based buffer overflow in the tg3_read_vpd function in drivers/net/ethernet/broadcom/tg3.c in the Linux kernel before 3.8.6 allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via crafted firmware that specifies a long string in the Vital Product Data (VPD) data

structure.

CVE-2013-1929 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

USN-1836-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu

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

[UBUNTU USN-1836-1](#)

[SECURITY] Fedora 18 Update: kernel-3.8.6-203.fc18

[lists.fedoraproject.org](#)
[text/html](#)

[FEDORA FEDORA-2013-5368](#)

kernel/git/torvalds/linux.git - Linux kernel source tree

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

[MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=715230a44310a8cf66fbf5a46f9a62a9b2de424](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)

[REDHAT RHSA-2013:1645](#)

	text/html Inactive Link Not Archived	
	www.kernel.org text/plain	 CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.8.6
[security-announce] SUSE-SU-2013:1473-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2013:1473
tg3: fix length overflow in VPD firmware parsing · torvalds/linux@715230a · GitHub	Exploit Patch github.com text/html	 CONFIRM github.com/torvalds/linux/commit/715230a44310a8cf66fbfb5a46f9a62a9b2de424
oss-security - Re: CVE Request: tg3 VPD firmware -> driver injection	www.openwall.com text/html	 MLIST [oss-security] 20130405 Re: CVE Request: tg3 VPD firmware -> driver injection
	Exploit cansecwest.com application/pdf	 MISC cansecwest.com/slides/2013/PrivateCore%20CSW%202013.pdf
USN-1834-1: Linux kernel (Quantal HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1834-1
USN-1838-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1838-1
Bug 949932 – CVE-2013-1929 Kernel: tg3: buffer overflow in VPD firmware parsing	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=949932
Support / Security / Advisories // MDVSA-2013:176 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2013:176
USN-1835-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1835-1
[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

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	Linux	Linux Kernel	3.8.0	All	All	All

Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	3.8.4	All	All	All
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	3.8.4	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:3.8.0:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.1:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.2:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.3:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.4:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.0:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.1:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.2:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.3:*****:.*:						
cpe:2.3:o:linux:linux_kernel:3.8.4:*****:.*:						
cpe:2.3:o:linux:linux_kernel:*****:.*:						

No vendor comments have been submitted for this CVE

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](#)