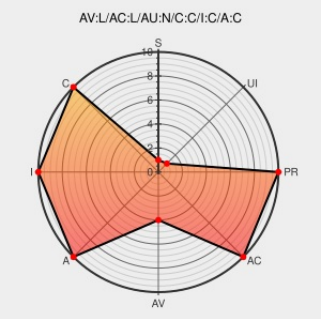
CVE-2013-2094

Published on: 05/14/2013 12:00:00 AM UTC

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

CVE-2013-2094

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



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

The perf_swevent_init function in kernel/events/core.c in the Linux kernel before 3.8.9 uses an incorrect integer data type, which allows local users to gain privileges via a crafted perf_event_open system call.

CVE-2013-2094 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch, 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=8176cced706b5e5d15887584150764894e94e02f
[security-announce] openSUSE-SU-2013:0951-1: critical: kernel: security	lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:0951
USN-1836-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com, text/html	UBUNTU USN-1836-1
Red Hat Customer Portal	access.redhat.com, text/html	MISC access.redhat.com/errata/RHSA-2013:0832

USN-1825-1: Linux kernel vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1825-1
USN-1828-1: Linux kernel (Quantal HWE) vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1828-1
Linux local privilege escalation 0day, 2.6.37 - 3.8.10 | Hacker News	news.ycombinator.com text/html	MISC news.ycombinator.com/item?id=5703758
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 93361
Ubuntu 12.04.0-2LTS x64 perf_swevent_init - Kernel Local Root Exploit	www.exploit-db.com Proof of Concept text/x-c	EXPLOIT-DB 33589
sd@fucksheep.org's semtex.c: Local Linux root exploit, 2.6.37-3.8.8 inclusive (and 2.6.32 on CentOS) 0-day : netsec	www.reddit.com text/html	MISC www.reddit.com/r/netsec/comments/1eb9iw
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0830
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0829
[security-announce] openSUSE-SU-2013:1042-1: critical: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1042
access.redhat.com | CVE-2013-2094	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2013-2094
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0925
Linux PERF_EVENTS Local Root ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/121616/semtex.c
Linux-Kernel Archive: Re: sw_perf_event_destroy() oops while fuzzing	lkml.indiana.edu text/html	MLIST [linux-kernel] 20130412 Re: sw_perf_event_destroy() oops while fuzzing
Dan Rosenberg na Twitterze: "For those following along, here's the fix: http://t.co/8Q3PzIL7IX"	Patch nitter.domain.glass text/html	MISC twitter.com/djrbliss/statuses/334301992648331267
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.8.9
[CentOS-announce] CentOS-6 CVE-2013-2094 Kernel Issue	lists.centos.org text/html	MLIST [CentOS-announce] 20130515 CentOS-6 CVE-2013-2094 Kernel Issue
Linux-Kernel Archive: sw_perf_event_destroy() oops while fuzzing	lkml.indiana.edu text/html	MLIST [linux-kernel] 20130412 sw_perf_event_destroy() oops while fuzzing

Bug 962792 – CVE-2013-2094 kernel: perf_swevent_enabled array out-of-bound access	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=962792
[CentOS-announce] CESA-2013:0830 Important CentOS 6 kernel Update	lists.centos.org text/html	MLIST [CentOS-announce] 20130517 CESA-2013:0830 Important CentOS 6 kernel Update
USN-1827-1: Linux kernel vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1827-1
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0840
USN-1838-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1838-1
Linux-Kernel Archive: Re: sw_perf_event_destroy() oops while fuzzing	lkml.indiana.edu text/x-c	MLIST [linux-kernel] 20130413 Re: sw_perf_event_destroy() oops while fuzzing
Support / Security / Advisories / / MDVSA-2013:176 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:176
[security-announce] SUSE-SU-2013:0819-1: critical: Security update for t	lists.opensuse.org text/html	SUSE SUSE-SU-2013:0819
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0841
[security-announce] openSUSE-SU-2013:0847-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0847
perf: Treat attr.config as u64 in perf_swevent_init() · torvalds/linux@8176cce · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/8176cced706b5e5d15887584150764894e94e02f
oss-security - Re: CVE Request: linux kernel perf out-of-bounds access	www.openwall.com text/html	MLIST [oss-security] 20130514 Re: CVE Request: linux kernel perf out-of-bounds access
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0830
USN-1826-1: Linux kernel vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1826-1

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2013-2094 exploit for android

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	3.8.5	All	All	All
Operating System	Linux	Linux Kernel	3.8.6	All	All	All
Operating System	Linux	Linux Kernel	3.8.7	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	3.8.5	All	All	All
Operating System	Linux	Linux Kernel	3.8.6	All	All	All
Operating System	Linux	Linux Kernel	3.8.7	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:3.8.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.7:*:*:*:*:*:*:*:

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:3.8.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.7:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→