



CVE-2013-0871

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

Summary

CVE	CVE-2013-0871
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-18 04:41:50 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Race condition in the ptrace functionality in the Linux kernel before 3.7.5 allows local users to gain privileges via a PTRACE

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

AV:L/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-362 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:N/C:C/I:C/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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-364	
USN-1737-1: Linux kernel (EC2) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-364	
USN-1740-1: Linux kernel (OMAP4) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-364	
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.7.5			af854a3a-2127-422b-91ae-364	
USN-1739-1: Linux kernel vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
USN-1745-1: Linux kernel (OMAP4) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
git.kernel.org			af854a3a-2127-422b-91ae-364	
USN-1742-1: Linux kernel (OMAP4) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
USN-1738-1: Linux kernel (Oneiric backport) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
USN-1744-1: Linux kernel vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
ptrace: ensure arch_ptrace/ptrace_request can never race with SIGKILL · torvalds/linux@9899d11 · GitHub			af854a3a-2127-422b-91ae-364	
911937 – (CVE-2013-0871) CVE-2013-0871 kernel: race condition with PTRACE_SETREGS			af854a3a-2127-422b-91ae-364	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-364	
oss-security - Linux kernel race condition with PTRACE_SETREGS (CVE-2013-0871)			af854a3a-2127-422b-91ae-364	
Debian -- Security Information -- DSA-2632-1 linux-2.6			af854a3a-2127-422b-91ae-364	
[security-announce] SUSE-SU-2013:0674-1: important: Security update for			af854a3a-2127-422b-91ae-364	
USN-1743-1: Linux kernel (Quantal HWE) vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
USN-1736-1: Linux kernel vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
USN-1741-1: Linux kernel vulnerability Ubuntu			af854a3a-2127-422b-91ae-364	
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security			af854a3a-2127-422b-91ae-364	
[security-announce] SUSE-SU-2013:0341-1: important: Security update for			af854a3a-2127-422b-91ae-364	
kernel/git/torvalds/linux.git - Linux kernel source tree			MITRE	
CVE Program record			CVE.ORG	
NVD vulnerability detail			NVD	
No vendor comments have been submitted for this CVE.				

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)