



CVE-2007-0006

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

Summary

CVE	CVE-2007-0006
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-06 19:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The key serial number collision avoidance code in the key_alloc_serial function in Linux kernel 2.6.9 up to 2.6.20 allows loc

Risk And Classification

Primary CVSS: v2.0 1.9 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All

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		Link
Ubuntu update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
USN-451-1: Linux kernel vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
227495 – CVE-2007-0006 Key serial number collision problem	af854a3a-2127-422b-91ae-364da2661108		bugzilla.redhat.com
Security Announcement	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
7727 – spinlock CPU recursion	af854a3a-2127-422b-91ae-364da2661108		bugzilla.redhat.com
Linux Kernel Key_Alloc_Serial() Local Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
Red Hat update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
Linux Kernel "key_alloc_serial()" Denial of Service - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
SUSE update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
rhnl.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
rPath update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
rhnl.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108		ubuntu.com
Mandriva update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108		ovalinux.org
issues.rpath.com/browse/RPL-1097	af854a3a-2127-422b-91ae-364da2661108		issues.rpath.com
rPath update for kernel and xen - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.com
Mandriva update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2661108		secunia.com
CVE Program record	CVE.ORG		www.cve.org
NVD vulnerability detail	NVD		nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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