



CVE-2010-3904

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-3904
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-06 20:13:00 UTC
Updated	2026-04-21 17:29:12 UTC
Description	The rds_page_copy_user function in net/rds/page.c in the Reliable Datagram Sockets (RDS) protocol implementation in the

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.014470000 probability, percentile 0.808150000 (date 2026-04-23)

CISA KEV: Listed on 2023-05-12; due 2023-06-02; ransomware use Unknown

Problem Types: CWE-1284 | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Improper Input Validation Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://lkml.iu.edu/hypermail/linux/kernel/1601.3/06474.html ; https://nvd.nist.gov/vuln/detail/CVE-2010-3904

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All

Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Vmware	Esxi	3.5	All	All	All
Operating System	Vmware	Esxi	4.0	All	All	All
Operating System	Vmware	Esxi	4.1	All	All	All
Operating System	Vmware	Esxi	5.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91
VSR 404 Not Found	af854a3a-2127-422b-91
Support	af854a3a-2127-422b-91
SecurityTracker.com Archives - Linux Kernel RDS Protocol Bug Lets Local Users Gain Elevated Privileges	af854a3a-2127-422b-91
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91
Bug 642896 – CVE-2010-3904 kernel: RDS sockets local privilege escalation	af854a3a-2127-422b-91
SecurityFocus	af854a3a-2127-422b-91
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b
VSR Security Advisories	af854a3a-2127-422b-91
USN-1000-1: Linux kernel vulnerabilities Ubuntu	af854a3a-2127-422b-91
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91
US-CERT Vulnerability Note VU#362983	af854a3a-2127-422b-91
About Secunia Research Flexera	af854a3a-2127-422b-91
VMSA-2011-0012.2	af854a3a-2127-422b-91
404: File not found	af854a3a-2127-422b-91
Linux 2.6.30 < 2.6.36-rc8 - Reliable Datagram Sockets (RDS) Privilege Escalation (Metasploit) - Linux local Exploit	af854a3a-2127-422b-91
vReliable Datagram Sockets (RDS) rds_npage_conv_user Privilege Escalation ~ Packet Storm	af854a3a-2127-422b-91

Vendor Catalog: CVEs (CVE) />_page_copy_desc />_privilege Escalation />_kernel Storm	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	af854a3a-2127-422b-91
Support	af854a3a-2127-422b-91
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2023-05-12T00:00:00.000Z	CVE-2010-3904 added to CISA KEV

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](#)