



CVE-2006-0744

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2006-0744
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-18 10:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Linux kernel before 2.6.16.5 does not properly handle uncanonical return addresses on Intel EM64T CPUs, which reports a

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

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

EPSS: 0.001060000 probability, percentile 0.285820000 (date 2026-04-20)

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All

Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All

Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.16.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.16_rc7	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All

Operating System	Linux	Linux Kernel	2.6.3	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc4	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	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
usn/usn-302-1 - Ubuntu: Linux for human beings	af854a3a-2127-422b-91ae-364da2661108	www.ubuntu.com
Mandriva update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da2661108	www.mandriva.com
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com
LWN: Fedora alert FEDORA-2006-423 (kernel)	af854a3a-2127-422b-91ae-364da2661108	lwn.net
Security Announcement	af854a3a-2127-422b-91ae-364da2661108	www.novell.com
Ubuntu update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da2661108	www.mandriva.com
Linux Kernel Program Control Return Denial of Service - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
404: File not found	af854a3a-2127-422b-91ae-364da2661108	kernel.org
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com
Red Hat update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Debian -- Security Information -- DSA-1103-1 kernel-source-2.6.8	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
www.osvdb.org/24639	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org
ASA-2006-161 (RHSA-2006-0493)	af854a3a-2127-422b-91ae-364da2661108	support.avaya.com
Linux Kernel Intel EM64T SYSRET Local Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org
Security Announcement	af854a3a-2127-422b-91ae-364da2661108	www.novell.com
SUSE update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
Security Announcement	af854a3a-2127-422b-91ae-364da2661108	www.novell.com
ASA-2006-180 (RHSA-2006-0437)	af854a3a-2127-422b-91ae-364da2661108	support.avaya.com
Fedora update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Red Hat update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
SUSE update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
Debian update for kernel-source-2.6.8 - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
SUSE update for kernel - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.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.

© [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](#)