



CVE-2005-0001

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2005-0001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	Race condition in the page fault handler (fault.c) for Linux kernel 2.2.x to 2.2.7, 2.4 to 2.4.29, and 2.6 to 2.6.10, when running

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.2.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.20	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All

Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.25	All	All	All
Operating System	Linux	Linux Kernel	2.4.26	All	All	All
Operating System	Linux	Linux Kernel	2.4.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.28	All	All	All
Operating System	Linux	Linux Kernel	2.4.29	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.2.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All

Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.20	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All
Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.25	All	All	All
Operating System	Linux	Linux Kernel	2.4.26	All	All	All
Operating System	Linux	Linux Kernel	2.4.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.28	All	All	All
Operating System	Linux	Linux Kernel	2.4.29	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All

Operating System	Hedhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Trustix	Secure Linux	2	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	2.2	All	All	All
Operating System	Trustix	Secure Linux	2	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	2.2	All	All	All

References

Reference

[Full-Disclosure] Linux kernel i386 SMP page fault handler privilege escalation

Debian -- Security Information -- DSA-1067-1 kernel-source-2.4.16

'Linux kernel i386 SMP page fault handler privilege escalation' - MARC

SecurityTracker.com Archives - Linux Kernel Multiprocessor Page Fault Handler Race Condition Lets Local Users Gain Elevated Privileges

Debian -- Security Information -- DSA-1070-1 kernel-source-2.4.19

isec.pl/vulnerabilities/isec-0022-pagefault.txt

Linux Kernel Symmetrical Multiprocessing Page Fault Local Privilege Escalation Vulnerability

rh.n.redhat.com | Red Hat Support

IBM X-Force Exchange

rh.n.redhat.com | Red Hat Support

Debian -- Security Information -- DSA-1082-1 kernel-source-2.4.17

rh.n.redhat.com | Red Hat Support

FLSA:2336

Advisories - Mandriva

2005-0001

rhn.redhat.com | Red Hat Support

Home - Conectiva

Secunia - Advisories - Debian update for kernel-source-2.4.18

'[USN-60-0] Linux kernel vulnerabilities' - MARC

Secunia - Advisories - Debian update for kernel-source-2.4.17

Repository / Oval Repository

Secunia - Advisories - Linux Kernel Page Fault Handler Privilege Escalation

Debian -- Security Information -- DSA-1069-1 kernel-source-2.4.18

Secunia - Advisories - Debian update for kernel-source-2.4.19

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report