CVE-2004-1058

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

Summary

CVE	CVE-2004-1058
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-10 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Race condition in Linux kernel 2.6 allows local users to read the environment variables of another process that is still spawn

Risk And Classification

Primary CVSS: v2.0 1.2 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

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	2.6.10	rc2	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	2.6.6	rc1	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	2.6.8	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	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All

Vendor Declared Affected Products

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

References

References

Reference
IBM X-Force Exchange
Secunia - Advisories - Red Hat update for kernel
Secunia - Advisories - Debian update for kernel-source-2.4.27
Linux Kernel Multiple Vulnerabilities - Advisories - Secunia
rhn.redhat.com | Red Hat Support
Secunia - Advisories - SUSE update for kernel
Gentoo Linux Documentation -- Linux Kernel: Multiple information leaks
SGI ProPack kernel Multiple Vulnerabilities - Advisories - Secunia
rhn.redhat.com | Red Hat Support
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: kernel various security problems (SUSE-SA:2006:0
152532 – Multiple kernel security problems: CAN-2005-0384, CAN-2005-0400, CAN-2005-0449, CAN-2005-0531(?), CAN-2005-0749, CAN-2
patches.sgi.com/support/free/security/advisories/20060402-01-U
Debian -- Security Information -- DSA-1018-2 kernel-source-2.4.27
Linux Kernel Process Spawning Race Condition Environment Variable Disclosure Vulnerability
Linux Kernel PROC Filesystem Local Information Disclosure Vulnerability
Advisories - Mandriva
rhn.redhat.com | Red Hat Support
USN-38-1: Linux kernel vulnerabilities | Ubuntu security notices
Repository / Oval Repository
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.

Free CVE JSON API cve.report/api

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