



# CVE-2004-0495

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

## Summary

<b>CVE</b>	CVE-2004-0495
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-08-06 04:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Multiple unknown vulnerabilities in Linux kernel 2.4 and 2.6 allow local users to gain privileges or access kernel memory, as

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Avaya</a>	<a href="#">Converged Communications Server</a>	2.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">Converged Communications Server</a>	2.0	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Intuity Audix</a>	All	All	ix	All
Application	<a href="#">Avaya</a>	<a href="#">Intuity Audix</a>	All	All	ix	All
Operating System	<a href="#">Avaya</a>	<a href="#">Modular Messaging Message Storage Server</a>	s3400	All	All	All
Operating System	<a href="#">Avaya</a>	<a href="#">Modular Messaging Message Storage Server</a>	s3400	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8300</a>	r2.0.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8300</a>	r2.0.1	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8300</a>	r2.0.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8300</a>	r2.0.1	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8500</a>	r2.0.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8500</a>	r2.0.1	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8500</a>	r2.0.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8500</a>	r2.0.1	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8700</a>	r2.0.0	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8700</a>	r2.0.1	All	All	All
Hardware	<a href="#">Avaya</a>	<a href="#">S8700</a>	r2.0.0	All	All	All

Hardware	Avaya	S8700	r2.0.1	All	All	All
Operating System	Conectiva	Linux	8.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Conectiva	Linux	8.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	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	2.4.21	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	2.6.0	All	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	2.6.2	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	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	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	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.2	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.3	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.4	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.5	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.6	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.6	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.7	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.7	rc1	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	advanced_servers	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	advanced_servers	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	workstation	All
Application	<a href="#">Suse</a>	<a href="#">Suse Email Server</a>	3.1	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Email Server</a>	iii	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Email Server</a>	3.1	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Email Server</a>	iii	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	7	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All

Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	7	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Admin-cd For Firewall</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Admin-cd For Firewall</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Connectivity Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Connectivity Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Database Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Database Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Firewall Cd</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Firewall Cd</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Office Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Office Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Office Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Office Server</a>	All	All	All	All

## References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Gentoo Linux Documentation -- Linux Kernel: Multiple vulnerabilities	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Vendor Advisory
MDKSA-2004:066	MANDRAKE	<a href="http://www.mandrakesecure.net">www.mandrakesecure.net</a>	
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>	
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>	
Home - Conectiva	CONNECTIVA	<a href="https://distro.conectiva.com.br">distro.conectiva.com.br</a>	
404 Page Not Found   SUSE	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
Linux Kernel Multiple Device Driver Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Patch, Vendor Adviso
LWN: Fedora alert FEDORA-2004-186 (kernel)	FEDORA	<a href="http://lwn.net">lwn.net</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	

Home - Conectiva	CONNECTIVA	<a href="http://distro.conectiva.com.br">distro.conectiva.com.br</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch, Vendor Advisc
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)**