



# CVE-2002-0004

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

## Summary

<b>CVE</b>	CVE-2002-0004
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2002-02-27 05:00:00 UTC
<b>Updated</b>	2017-10-10 01:30:00 UTC
<b>Description</b>	Heap corruption vulnerability in the "at" program allows local users to execute arbitrary code via a malformed execution time

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Caldera</a>	<a href="#">Openlinux Server</a>	3.1	All	All	All
Application	<a href="#">Caldera</a>	<a href="#">Openlinux Server</a>	3.1	All	All	All
Application	<a href="#">Caldera</a>	<a href="#">Openlinux Workstation</a>	3.1	All	All	All
Application	<a href="#">Caldera</a>	<a href="#">Openlinux Workstation</a>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.2	All	sparc	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.1.1	All	All	All

Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.2	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.3	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.4	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.1.1	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.2	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.3	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	4.4	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.0	All	ppc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.1	All	ia64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.0	All	ppc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	8.1	All	ia64	All
Operating System	<a href="#">Netbsd</a>	<a href="#">Netbsd</a>	1.5.2	All	All	All
Operating System	<a href="#">Netbsd</a>	<a href="#">Netbsd</a>	1.5.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	sparc	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.1	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.1	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.1	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.2	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.2	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.2	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	6.2	All	sparc	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.1	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.1	All	i386	All

Operating System	Redhat	Linux	7.1	All	ia64	All
Operating System	Redhat	Linux	7.2	All	alpha	All
Operating System	Redhat	Linux	7.2	All	i386	All
Operating System	Redhat	Linux	7.2	All	ia64	All
Operating System	Slackware	Slackware Linux	7.0	All	All	All
Operating System	Slackware	Slackware Linux	7.1	All	All	All
Operating System	Slackware	Slackware Linux	8.0	All	All	All
Operating System	Slackware	Slackware Linux	7.0	All	All	All
Operating System	Slackware	Slackware Linux	7.1	All	All	All
Operating System	Slackware	Slackware Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	6.4	All	i386	All
Operating System	Suse	Suse Linux	6.4	All	ppc	All
Operating System	Suse	Suse Linux	6.4	alpha	All	All
Operating System	Suse	Suse Linux	7.0	All	i386	All
Operating System	Suse	Suse Linux	7.0	All	ppc	All
Operating System	Suse	Suse Linux	7.0	All	sparc	All
Operating System	Suse	Suse Linux	7.0	alpha	All	All
Operating System	Suse	Suse Linux	7.1	All	ppc	All
Operating System	Suse	Suse Linux	7.1	All	sparc	All
Operating System	Suse	Suse Linux	7.1	All	x86	All
Operating System	Suse	Suse Linux	7.1	alpha	All	All
Operating System	Suse	Suse Linux	7.2	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	ppc	All
Operating System	Suse	Suse Linux	7.3	All	sparc	All
Operating System	Suse	Suse Linux	6.4	All	i386	All
Operating System	Suse	Suse Linux	6.4	All	ppc	All
Operating System	Suse	Suse Linux	6.4	alpha	All	All
Operating System	Suse	Suse Linux	7.0	All	i386	All
Operating System	Suse	Suse Linux	7.0	All	ppc	All
Operating System	Suse	Suse Linux	7.0	All	sparc	All
Operating System	Suse	Suse Linux	7.0	alpha	All	All
Operating System	Suse	Suse Linux	7.1	All	ppc	All
Operating System	Suse	Suse Linux	7.1	All	sparc	All
Operating System	Suse	Suse Linux	7.1	All	x86	All

Operating System	Suse	Suse Linux	7.1	alpha	All	All
Operating System	Suse	Suse Linux	7.2	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	ppc	All
Operating System	Suse	Suse Linux	7.3	All	sparc	All

## References

Reference	Source	Link	Tags
"/usr/bin/at 31337 + vuln' problem + exploit' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
HPSBTL0302-034	HP	<a href="http://online.securityfocus.com">online.securityfocus.com</a>	
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
'MDKSA-2002:007 - at update' - MARC	MANDRAKE	<a href="http://marc.info">marc.info</a>	
AT Maliciously Formatted Time Heap Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit, P
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch, Ve
Debian -- Security Information -- DSA-102-2 at	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Patch
SecurityFocus HOME Advisories: Heap corruption vulnerability in the at package	HP	<a href="http://online.securityfocus.com">online.securityfocus.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
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

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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

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