CVE-2002-0004

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2002-0004
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-02-27 05:00:00 UTC
Updated	2017-10-10 01:30:00 UTC
Description	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	Caldera	Openlinux Server	3.1	All	All	All
Application	Caldera	Openlinux Server	3.1	All	All	All
Application	Caldera	Openlinux Workstation	3.1	All	All	All
Application	Caldera	Openlinux Workstation	3.1	All	All	All
Operating System	Debian	Debian Linux	2.2	All	68k	All
Operating System	Debian	Debian Linux	2.2	All	alpha	All
Operating System	Debian	Debian Linux	2.2	All	arm	All
Operating System	Debian	Debian Linux	2.2	All	ia-32	All
Operating System	Debian	Debian Linux	2.2	All	powerpc	All
Operating System	Debian	Debian Linux	2.2	All	sparc	All
Operating System	Debian	Debian Linux	2.2	All	68k	All
Operating System	Debian	Debian Linux	2.2	All	alpha	All
Operating System	Debian	Debian Linux	2.2	All	arm	All
Operating System	Debian	Debian Linux	2.2	All	ia-32	All
Operating System	Debian	Debian Linux	2.2	All	powerpc	All
Operating System	Debian	Debian Linux	2.2	All	sparc	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All

Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	ia64	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	ia64	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Redhat	Linux	6.2	All	alpha	All
Operating System	Redhat	Linux	6.2	All	i386	All
Operating System	Redhat	Linux	6.2	All	sparc	All
Operating System	Redhat	Linux	7.0	All	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.1	All	alpha	All
Operating System	Redhat	Linux	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	Redhat	Linux	6.2	All	alpha	All
Operating System	Redhat	Linux	6.2	All	i386	All
Operating System	Redhat	Linux	6.2	All	sparc	All
Operating System	Redhat	Linux	7.0	All	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.1	All	alpha	All
Operating System	Redhat	Linux	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	marc.info	
HPSBTL0302-034	HP	online.securityfocus.com	
Security Announcement	SUSE	www.novell.com	
'MDKSA-2002:007 - at update' - MARC	MANDRAKE	marc.info	
AT Maliciously Formatted Time Heap Overflow Vulnerability	BID	www.securityfocus.com	Exploit, P
redhat.com | Red Hat Support	REDHAT	www.redhat.com	Patch, Ve
Debian -- Security Information -- DSA-102-2 at	DEBIAN	www.debian.org	Patch
SecurityFocus HOME Advisories: Heap corruption vulnerability in the at package	HP	online.securityfocus.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.