CVE-2004-0996

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

Summary

CVE	CVE-2004-0996
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	main.c in cscope 15-4 and 15-5 creates temporary files with predictable filenames, which allows local users to overwrite arb

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cscope	Cscope	13.0	All	All	All

Application	Cscope	Cscope	15.1	All	All	All
Application	Cscope	Cscope	15.3	All	All	All
Application	Cscope	Cscope	15.4	All	All	All
Application	Cscope	Cscope	15.5	All	All	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-32	All
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Sco	Unixware	7.1.1	All	All	All
Operating System	Sco	Unixware	7.1.3	All	All	All
Operating System	Sco	Unixware	7.1.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
APPLE-SA-2007-07-31 Security Update 2007-007	af854a3a-2127-422b-91ae-364da2661108	lists.apple.com
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforc
Apple Mac OS X 2007-007 Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
About Security Update 2007-007	af854a3a-2127-422b-91ae-364da2661108	docs.info.apple
Cscope Insecure Temporary File Creation Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.co

Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.co
Gentoo Linux Documentation -- Cscope: Insecure creation of temporary files	af854a3a-2127-422b-91ae-364da2661108	www.gentoo.or
Debian -- Security Information -- DSA-610-1 cscope	af854a3a-2127-422b-91ae-364da2661108	www.debian.or
'STG Security Advisory: [SSA-20041122-09] cscope insecure temp' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-04-09	Mark J Cox	Not vulnerable. cscope packages shipped with Red Hat Enterprise Linux 3, 4, and 5 contain a ba

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