



CVE-2004-0523

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

Summary

CVE	CVE-2004-0523
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-18 04:00:00 UTC
Updated	2020-01-21 15:47:00 UTC
Description	Multiple buffer overflows in krb5_aname_to_localname for MIT Kerberos 5 (krb5) 1.3.3 and earlier allow remote attackers to

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos	1.0	All	All	All
Application	Mit	Kerberos	1.0.8	All	All	All
Application	Mit	Kerberos	1.2.2.beta1	All	All	All
Application	Mit	Kerberos	1.0	All	All	All
Application	Mit	Kerberos	1.0.8	All	All	All
Application	Mit	Kerberos	1.2.2.beta1	All	All	All
Application	Mit	Kerberos 5	1.0	All	All	All
Application	Mit	Kerberos 5	1.0.6	All	All	All
Application	Mit	Kerberos 5	1.1	All	All	All
Application	Mit	Kerberos 5	1.1.1	All	All	All
Application	Mit	Kerberos 5	1.2	All	All	All
Application	Mit	Kerberos 5	1.2	beta1	All	All
Application	Mit	Kerberos 5	1.2	beta2	All	All
Application	Mit	Kerberos 5	1.2.1	All	All	All
Application	Mit	Kerberos 5	1.2.2	All	All	All
Application	Mit	Kerberos 5	1.2.3	All	All	All
Application	Mit	Kerberos 5	1.2.4	All	All	All

Application	Mit	Kerberos 5	1.2.5	All	All	All
Application	Mit	Kerberos 5	1.2.6	All	All	All
Application	Mit	Kerberos 5	1.2.7	All	All	All
Application	Mit	Kerberos 5	1.3	All	All	All
Application	Mit	Kerberos 5	1.3	alpha1	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.0	All	All	All
Application	Mit	Kerberos 5	1.0.6	All	All	All
Application	Mit	Kerberos 5	1.1	All	All	All
Application	Mit	Kerberos 5	1.1.1	All	All	All
Application	Mit	Kerberos 5	1.2	All	All	All
Application	Mit	Kerberos 5	1.2	beta1	All	All
Application	Mit	Kerberos 5	1.2	beta2	All	All
Application	Mit	Kerberos 5	1.2.1	All	All	All
Application	Mit	Kerberos 5	1.2.2	All	All	All
Application	Mit	Kerberos 5	1.2.3	All	All	All
Application	Mit	Kerberos 5	1.2.4	All	All	All
Application	Mit	Kerberos 5	1.2.5	All	All	All
Application	Mit	Kerberos 5	1.2.6	All	All	All
Application	Mit	Kerberos 5	1.2.7	All	All	All
Application	Mit	Kerberos 5	1.3	All	All	All
Application	Mit	Kerberos 5	1.3	alpha1	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All
Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All
Application	Sun	Seam	1.0	All	All	All
Application	Sun	Seam	1.0.1	All	All	All
Application	Sun	Seam	1.0.2	All	All	All
Application	Sun	Seam	1.0	All	All	All
Application	Sun	Seam	1.0.1	All	All	All
Application	Sun	Seam	1.0.2	All	All	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All

Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Sunos	5.8	All	All	All
Operating System	Sun	Sunos	5.8	All	All	All
Application	Tinysofa	Tinysofa Enterprise Server	1.0	All	All	All
Application	Tinysofa	Tinysofa Enterprise Server	1.0_u1	All	All	All
Application	Tinysofa	Tinysofa Enterprise Server	1.0	All	All	All
Application	Tinysofa	Tinysofa Enterprise Server	1.0_u1	All	All	All

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisecurity.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
US-CERT Vulnerability Note VU#686862	CERT-VN	www.kb.cert.org
MIT Kerberos 5 KRB5_AName_To_Localname Multiple Principal Name Buffer Overrun Vulnerabilities	BID	www.securityfocus.com
Debian -- Security Information -- DSA-520-1 krb5	DEBIAN	www.debian.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
20040604-01-U	SGI	patches.sgi.com
20040605-01-U	SGI	patches.sgi.com
Gentoo Linux Documentation -- mit-krb5: Multiple buffer overflows in krb5_aname_to_localname	GENTOO	www.gentoo.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Home - Conectiva	CONNECTIVA	distro.conectiva.com.br
MDKSA-2004:056	MANDRAKE	www.mandrakesecurity.org
redhat.com Red Hat Support	REDHAT	www.redhat.com
101512	SUNALERT	sunsolve.sun.com
LWN: Fedora alert FEDORA-2004-149 (krb5)	FEDORA	lwn.net
'MITKRB5-SA-2004-001: buffer overflows in krb5_aname_to_localname' - MARC	BUGTRAQ	marc.info
'TSLSA-2004-0032 - kerberos' - MARC	TRUSTIX	marc.info
'TSSA-2004-009 - kerberos5' - MARC	BUGTRAQ	marc.info
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

No vendor comments have been submitted for this CVE.

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)