



CVE-2010-1323

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

Summary

CVE	CVE-2010-1323
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-02 16:22:00 UTC
Updated	2020-01-21 15:46:00 UTC
Description	MIT Kerberos 5 (aka krb5) 1.3.x, 1.4.x, 1.5.x, 1.6.x, 1.7.x, and 1.8.x through 1.8.3 does not properly determine the acceptat

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos	5-1.5.4	All	All	All
Application	Mit	Kerberos	5-1.5.4	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	1.3.1	All	All	All
Application	Mit	Kerberos 5	1.3.2	All	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.3.4	All	All	All
Application	Mit	Kerberos 5	1.3.5	All	All	All
Application	Mit	Kerberos 5	1.3.6	All	All	All
Application	Mit	Kerberos 5	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All
Application	Mit	Kerberos 5	1.4.2	All	All	All
Application	Mit	Kerberos 5	1.4.3	All	All	All
Application	Mit	Kerberos 5	1.4.4	All	All	All
Application	Mit	Kerberos 5	1.5	All	All	All
Application	Mit	Kerberos 5	1.5.1	All	All	All

Application	Mit	Kerberos 5	1.5.2	All	All	All
Application	Mit	Kerberos 5	1.5.3	All	All	All
Application	Mit	Kerberos 5	1.6	All	All	All
Application	Mit	Kerberos 5	1.6.1	All	All	All
Application	Mit	Kerberos 5	1.6.2	All	All	All
Application	Mit	Kerberos 5	1.7	All	All	All
Application	Mit	Kerberos 5	1.7.1	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	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	1.3.1	All	All	All
Application	Mit	Kerberos 5	1.3.2	All	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.3.4	All	All	All
Application	Mit	Kerberos 5	1.3.5	All	All	All
Application	Mit	Kerberos 5	1.3.6	All	All	All
Application	Mit	Kerberos 5	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All
Application	Mit	Kerberos 5	1.4.2	All	All	All
Application	Mit	Kerberos 5	1.4.3	All	All	All
Application	Mit	Kerberos 5	1.4.4	All	All	All
Application	Mit	Kerberos 5	1.5	All	All	All
Application	Mit	Kerberos 5	1.5.1	All	All	All
Application	Mit	Kerberos 5	1.5.2	All	All	All
Application	Mit	Kerberos 5	1.5.3	All	All	All
Application	Mit	Kerberos 5	1.6	All	All	All
Application	Mit	Kerberos 5	1.6.1	All	All	All
Application	Mit	Kerberos 5	1.6.2	All	All	All
Application	Mit	Kerberos 5	1.7	All	All	All
Application	Mit	Kerberos 5	1.7.1	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All

Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
References						
Reference						
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001						
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:023						
MIT Kerberos Checksum Handling Errors May Let Remote or Remote Authenticated Users Forge/Modify Certain Data - SecurityTracker						
Support						
VMSA-2011-0007						
SecurityFocus						
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						
Oracle Critical Patch Update - July 2015						
SecurityFocus						
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						
MIT Kerberos 5 1.3.x Checksum Multiple Remote Security Bypass Vulnerabilities						
USN-1030-1: Kerberos vulnerabilities Ubuntu						
SecurityFocus						
VMware KB: VMware ESXi 4.1 Patch ESXi410-201104401-SG: Updates Firmware						
'[security bulletin] HPSBUX02623 SSRT100355 rev.1 - HP-UX Running Kerberos, Remote Unauthorized Modif' - MARC						
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:024						
HP-UX update for Kerberos - Advisories - Community						
[Security-announce] VMSA-2011-0007 VMware ESXi and ESX Denial of Service and third party updates for Likewise components and ESX S						
Security Alerts - Secunia						
[SECURITY] Fedora 14 Update: krb5-1.8.2-7.fc14						
[security-announce] SUSE-SU-2012:0010-1: important: Security update for						
69610						
[security-announce] SUSE-SU-2012:0042-1: important: Security update for						
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						
VMSA-2011-0012.2						
Red Hat update for krb5 - Secunia.com						
[SECURITY] Fedora 13 Update: krb5-1.7.1-16.fc13						
Repository / Oval Repository						
Security Alerts - Secunia						
About the security content of Mac OS X v10.6.7 and Security Update 2011-001						
About Secunia Research Flexera						

Debian -- Security Information -- DSA-2129-1 krb5
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-007.txt
Support / Security / Advisories / / MDVSA-2010:246 Mandriva
Support / Security / Advisories / / MDVSA-2010:245 Mandriva
'[security bulletin] HPSBOV02682 SSRT100495 rev.1 - HP OpenVMS running Kerberos, Remote Denial of Ser' - MARC
Support
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report