

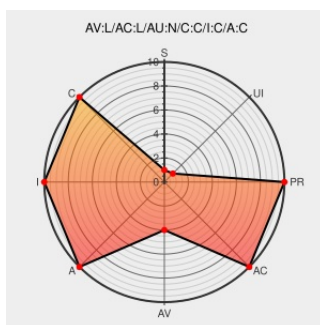


CVE-2004-1189

Published on: 12/31/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-1189

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kerberos 5](#) from [Mit](#) contain the following vulnerability:

The `add_to_history` function in `svr_principal.c` in `libkadm5srv` for MIT Kerberos 5 (`krb5`) up to 1.3.5, when performing a password change, does not properly track the password policy's history count and the maximum number of keys, which can cause an array index out-of-bounds error and may allow authenticated users to execute arbitrary code via a heap-based buffer overflow.

CVE-2004-1189 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Broken Link

www.trustix.org

text/plain

Inactive Link Not Archived

[TRUSTIX 2004-0069](#)

Repository / Oval Repository

Broken Link

Third Party Advisory

oval.cisecurity.org

text/html

[OVAL oval:org.mitre.oval:def:11911](#)

IBM X-Force Exchange

Third Party Advisory

VDB Entry

exchange.xforce.ibmcloud.com

text/html

[XF kerberos-libkadm5srv-bo\(18621\)](#)

	text/html	
Home - Conectiva	Broken Link distro.conectiva.com.br text/html	 CONECTIVA CLA-2005:917
Advisories - Mandriva	Third Party Advisory www.mandriva.com text/html	 MANDRAKE MDKSA-2004:156
Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2005:012
	Patch Vendor Advisory web.mit.edu text/plain	 CONFIRM web.mit.edu/kerberos/advisories/MITKRB5-SA-2004-004-pwhist.txt
'MITKRB5-SA-2004-004: heap overflow in libkadm5srv' - MARC	Issue Tracking Mailing List Third Party Advisory marc.info text/html	 BUGTRAQ 20041220 MITKRB5-SA-2004-004: heap overflow in libkadm5srv
'[USN-58-1] MIT Kerberos server vulnerability' - MARC	Issue Tracking Mailing List Third Party Advisory marc.info text/html	 BUGTRAQ 20050110 [USN-58-1] MIT Kerberos server vulnerability
Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2005:045
APPLE-SA-2005-08-17 Security Update 2005-007 v1.1	Mailing List Third Party Advisory lists.apple.com text/html	 APPLE APPLE-SA-2005-08-17
APPLE-SA-2005-08-15 Security Update 2005-007	Mailing List Third Party Advisory lists.apple.com text/html	 APPLE APPLE-SA-2005-08-15

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	All	All	All	All
cpe:2.3:a:mit:kerberos_5:*****:*						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#)