

# MITKRB5-SA-2008-001: double-free, uninitialized data vulnerabilities in krb5kdc

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00234.html>

---

- *From:* [raeburn@xxxxxxx](mailto:raeburn@xxxxxxx)
  - *Date:* Tue, 18 Mar 2008 14:14:53 -0400 (EDT)
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

MITKRB5-SA-2008-001

MIT krb5 Security Advisory 2008-001

Original release: 2008-03-18

Last update: 2008-03-18

Topic: double-free, uninitialized data vulnerabilities in krb5kdc

CVE-2008-0062

VU#895609

Use of a null or dangling pointer in the MIT Kerberos KDC can result in a crash or double-free, and may leak portions of process memory to an attacker.

CVSSv2 Vector: AV:N/AC:M/Au:N/C:P/I:P/A:C/E:P/RL:O/RC:C

CVSSv2 Base Score: 9.3

Access Vector: Network

Access Complexity: Medium

Authentication: None

Confidentiality Impact: Complete

Integrity Impact: Complete

Availability Impact: Complete

CVSSv2 Temporal Score: 6.5

Exploitability: Proof-of-Concept

Remediation Level: Official Fix

Report Confidence: Confirmed

CVE-2008-0063

VU#895609

Uninitialized stack values cause re-use of a small window of previous

stack values to be interpreted as message content. Some of the "content" may be returned to the attacker as part of an error response.

CVSSv2 Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:P/RL:O/RC:C

CVSSv2 Base Score: 4.3

Access Vector: Network  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None

CVSSv2 Temporal Score: 3.4

Exploitability: Proof-of-Concept  
Remediation Level: Official Fix  
Report Confidence: Confirmed

## SUMMARY

=====

When Kerberos 4 support is enabled in the MIT Kerberos 5 KDC, malformed messages may trigger two bugs:

CVE-2008-0062: A global variable holding a pointer to the message to be sent back to the client is only set for two recognized krb4 message types, but may be used (and freed) in additional cases, resulting in use of a null or dangling pointer.

CVE-2008-0063: The incoming krb4 message is copied into a fixed-size buffer on the stack, but the remainder of the buffer is left untouched, and the bounds checks use the size of the buffer, not the size of the data copied into it.

By default, Kerberos 4 support is compiled in but not enabled in recent versions, and these bugs are not exposed unless Kerberos 4 support is enabled.

These are implementation bugs, not protocol defects.

## IMPACT

=====

CVE-2008-0062: An unauthenticated remote attacker may cause a krb4-enabled KDC to crash, expose information, or execute arbitrary code. Successful exploitation of this vulnerability could compromise the Kerberos key database and host security on the KDC host.

## MITKRB5-SA-2008-001: double-free, uninitialized data vulnerabilities in krb5kdc

CVE-2008-0063: An unauthenticated remote attacker may cause a krb4-enabled KDC to expose information. It is theoretically possible for the exposed information to include secret key data on some platforms.

### AFFECTED SOFTWARE

=====

MIT Kerberos 5 version 1.6.3 KDC, and probably all earlier versions, when krb4 support is compiled in and enabled. (The krb4 support is disabled by default in recent releases.) No client or application server programs are affected.

### FIXES

=====

\* Apply the patch available at:

<http://web.mit.edu/kerberos/advisories/2008-001-patch.txt>

or in PGP-signed form at:

<http://web.mit.edu/kerberos/advisories/2008-001-patch.txt.asc>

\* These bugs will be fixed in the next release.

### REFERENCES

=====

This announcement is posted at:

<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2008-001.txt>

This announcement and related security advisories may be found on the MIT Kerberos security advisory page at:

<http://web.mit.edu/kerberos/advisories/index.html>

The main MIT Kerberos web page is at:

<http://web.mit.edu/kerberos/index.html>

CVSSv2:

<http://www.first.org/cvss/cvss-guide.html>

<http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

CVE: CVE-2008-0062 CVE-2008-0063

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0062>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0063>

CERT: VU#895609

<http://www.kb.cert.org/vuls/id/895609>

## CONTACT

=====

The MIT Kerberos Team security contact address is <krbcore-security@xxxxxxx>. When sending sensitive information, please PGP-encrypt it using the following key:

```
pub 1024D/2915318C 2008-01-18 [expires: 2009-02-01]
uid MIT Kerberos Team Security Contact <krbcore-security@xxxxxxx>
sub 2048g/3A91A276 2008-01-18 [expires: 2009-02-01]
```

## DETAILS

=====

CVE-2008-0062: If a bogus Kerberos 4 message (i.e., a message with the first byte having the value 4, but the second byte not describing one of the message types supported by the KDC) is received by the KDC, and there has been no previous Kerberos 4 traffic, a null pointer dereference will result, likely crashing the KDC. If there has been valid Kerberos 4 traffic already, a dangling pointer will be used to locate the message to send to the client; it may resend a previously generated response, send some other arbitrary chunk of process memory, perhaps including secret key data, or crash the process by attempting to access an invalid address. If the process doesn't crash, random addresses will be passed to free(), likely corrupting the free pool, and potentially leading to later crashes, data corruption, jumps to arbitrary locations in process memory, etc.

The KDC normally runs without write access to its database, so it is not likely to corrupt the database, except insofar as arbitrary code execution could theoretically corrupt anything the process has access to on the system.

CVE-2008-0063: If a Kerberos 4 message is truncated, previous contents of the stack may be used in place of the missing portions of the message. (Note that if the message type is missing, and the data read from the stack is not a recognized message type, this may indirectly trigger CVE-2008-0062 described above.) Several strings are read from the "message" as parts of principal names; these strings are limited to 40 bytes or the next ASCII NUL found in the buffer. If the KDC returns an error message indicating that a principal name is not found in its database, the principal name is included in the error message, and some of the old stack content may be there.

If the previously handled message was a valid Kerberos 4 message, parts of that message may be re-used for the new message; this wouldn't expose any data that wouldn't have been visible on the local network.

If the previously handled message was a Kerberos 5 message, the values overlaid by the buffer are likely to be old argument pointers, saved

registers, return addresses, and so forth. However, since stack contents and layout are highly dependent on the platform and compiler, it is impossible to assert that no secret key data may be leaked into the exposed stack regions on any platform.

REVISION HISTORY

=====

2008-03-18 original release

Copyright (C) 2008 Massachusetts Institute of Technology

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.7 (Darwin)

iD8DBQFH4AC6UqOaDMQ+e5gRAt5BAKCKfIKFE6assZ+fhbf8ghT5PsS5RQCfcQAJ  
MmnThImfNYzxigqYCX+Fkm8=  
=zmzD

-----END PGP SIGNATURE-----