

# [UNIX] Double-Free Vulnerability in Kadmind (Via GSS-API Library)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00010.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 4 Apr 2007 16:54:57 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Double-Free Vulnerability in Kadmind (Via GSS-API Library)

---

## SUMMARY

The MIT krb5 Kerberos administration daemon (kadmind) is vulnerable to a double-free attack in the RPCSEC\_GSS authentication flavor of the RPC library, which itself results from a bug in the GSS-API library. Under some error conditions, the krb5 GSS-API mechanism can free a buffer which an application may then free again. This may result in arbitrary code execution. Third-party applications using the GSS-API library provided with MIT krb5 may also be vulnerable.

Exploitation of double-free bugs is believed to be difficult.

This is a bug in the GSS-API library included with MIT krb5, which is used by kadmind and by some third-party applications. It is not a bug in the Kerberos protocol.

## DETAILS

Vulnerable Systems:

- \* kadmind from MIT releases krb5-1.4 through krb5-1.6
- \* third-party applications calling the RPC library included in MIT

## [UNIX] Double-Free Vulnerability in Kadmind (Via GSS-API Library)

releases krb5-1.4 through krb5-1.6

\* kadmind and third-party applications calling the RPC library in MIT releases earlier than krb5-1.4 may not be vulnerable because the RPCSEC\_GSS authentication flavor was not implemented in those RPC libraries.

\* third-party applications calling the GSS-API library included in any MIT krb5 releases, up to and including krb5-1.6, if the application handles GSS-API errors in a certain way

Immune Systems:

\* kadmind from MIT releases krb5-1.6.1

Impact:

An authenticated user may be able to cause a host running kadmind to execute arbitrary code.

Successful exploitation can compromise the Kerberos key database and host security on the host running these programs. (kadmind and the KDC typically run as root.) Unsuccessful exploitation attempts will likely result in the affected program crashing.

Third-party applications calling either the RPC library or the GSS-API library provided with MIT krb5 may be vulnerable.

Fixes:

\* The upcoming krb5-1.6.1 release will contain a fix for this vulnerability.

Prior to that release you may:

\* apply the patch

Note that releases prior to krb5-1.3 will require a different patch due to an additional related vulnerability in the same file.

This patch is also available at:

<<http://web.mit.edu/kerberos/advisories/2007-003-patch.txt>>

<http://web.mit.edu/kerberos/advisories/2007-003-patch.txt>

A PGP-signed patch is available at

<<http://web.mit.edu/kerberos/advisories/2007-003-patch.txt.asc>>

<http://web.mit.edu/kerberos/advisories/2007-003-patch.txt.asc>

```
*** src/lib/gssapi/krb5/k5unseal.c (revision 19510)
```

```
---- src/lib/gssapi/krb5/k5unseal.c (revision 19511)
```

```
*****
```

```
*** 457,464 ***
```

```
if ((ctx->initiate && direction != 0xff) ||
    (!ctx->initiate && direction != 0)) {
! if (toktype == KG_TOK_SEAL_MSG)
```

## [UNIX] Double-Free Vulnerability in Kadmind (Via GSS-API Library)

```
xfree(token.value);
*minor_status = G_BAD_DIRECTION;
return(GSS_S_BAD_SIG);
}
---- 457,467 ----

if ((ctx->initiate && direction != 0xff) ||
(!ctx->initiate && direction != 0)) {
! if (toktype == KG_TOK_SEAL_MSG) {
xfree(token.value);
+ message_buffer->value = NULL;
+ message_buffer->length = 0;
+ }
*minor_status = G_BAD_DIRECTION;
return(GSS_S_BAD_SIG);
}
```

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1216>>  
CVE-2007-1216

### Technical Details:

The `kg_unseal_v1()` function in `src/lib/gssapi/krb5/k5unseal.c` frees memory allocated for the "message\_buffer" `gss_buffer_t` when it detects an invalid direction encoding on the message. It does not set the pointer to `NULL`, nor does it set the length to zero. An application subsequently calling `gss_release_buffer()` on this `gss_buffer_t` will cause memory to be freed twice.

Much code provided with MIT `krb5` does not attempt to call `gss_release_buffer()` when `gss_unseal()` or `gss_unwrap()` fails, even though the GSS-API C-bindings specification permits it to do so. The `RPCSEC_GSS` authentication flavor for the RPC library, introduced in `krb5-1.4`, does call `gss_release_buffer()` when `gss_unwrap()` fails. This allows an authenticated attacker to trigger a double-free situation.

Third-party applications calling the RPC library provided with MIT `krb5` and using the `RPCSEC_GSS` authentication flavor are vulnerable. Third-party applications calling the MIT GSS-API library are vulnerable if they call `gss_release_buffer()` when they experience errors from `gss_unseal()` or `gss_unwrap()`.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:tlyu@xxxxxxx>> Tom Yu.  
The original article can be found at:  
<<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2007-003.txt>>  
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2007-003.txt>

[UNIX] Double-Free Vulnerability in Kadmind (Via GSS-API Library)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.