



June 26, 2007

---

McAfee, Inc.  
McAfee® Avert® Labs Security Advisory  
Public Release Date: 2007-06-26

## MIT Kerberos RPC library stack based memory corruption vulnerability

CVE-2007-2443

---

- **Synopsis**

An unauthenticated remote 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 typically runs as root.) Unsuccessful exploitation attempts will likely result in the affected program crashing.

Third-party applications calling the RPC library provided with MIT krb5 may be vulnerable. Other RPC libraries derived from SunRPC may be vulnerable.

---

- **Vulnerable System or Application**

- Kadmind from MIT releases up to and including krb5-1.6.1
- Third-party applications calling the RPC library included in MIT releases up to and including krb5-1.6.1

---

- **Vulnerability Information**

A signedness error exists within the "gssrpc\_\_svcauth\_unix()" function in the RPC library, which is used by kadmind and possibly other third-party products. This can be exploited to cause a stack-based buffer overflow. Exploitation of this vulnerability to lead to execution of arbitrary code is believed to be difficult.

---

- **Resolution**

krb5-1.6.2 fixes this vulnerability

---

- **Credits**

This vulnerability was discovered by Wei Wang of McAfee Avert Labs.

---

- **Legal Notice**

Copyright (C) 2007 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.