From: US-CERT Technical Alerts <technical-alerts@us-cert.gov>
To: technical-alerts@us-cert.gov
Subject: US-CERT Technical Cyber Security Alert TA07-177A -- MIT Kerberos Vulnerabilities
Date: Tue, 26 Jun 2007 16:30:49 -0400

National Cyber Alert System

Technical Cyber Security Alert TA07-177A

MIT Kerberos Vulnerabilities

Original release date: June 26, 2007
Last revised: --
Source: US-CERT

Systems Affected

* MIT Kerberos

Other products that use the RPC library provided with MIT Kerberos or other RPC libraries derived from SunRPC may also be affected.

Overview

The MIT Kerberos 5 implementation contains several vulnerabilities. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system.

I. Description

There are three vulnerabilities that affect MIT Kerberos 5:

* VU#356961 - MIT Kerberos RPC library gssrpc__svcauth_gssapi() uninitialized pointer free vulnerability

  A vulnerability in the MIT Kerberos administration daemon (kadmind) may allow an uninitialized pointer to be freed, which may allow a remote, unauthenticated user to execute arbitrary code. This vulnerability can be triggered by sending a specially crafted Kerberos message to a vulnerable system.

* VU#365313 - MIT Kerberos kadmind RPC library gssrpc__svcauth_unix() integer conversion error

  An integer conversion error vulnerability exists in the MIT Kerberos kadmind that may allow a remote, unauthenticated user to execute arbitrary code.

* VU#554257 - MIT Kerberos kadmind principal renaming stack buffer overflow

  A stack buffer overflow exists in the way the MIT Kerberos kadmind handles the principle renaming operation, which may allow a remote, authenticated user to execute arbitrary code.

II. Impact

A remote, unauthenticated attacker may be able to execute arbitrary code on KDCs, systems running kadmind, and application servers that

use the RPC library. An attacker could also cause a denial of service
on any of these systems. These vulnerabilities could result in the
compromise of both the KDC and an entire Kerberos realm.

III. Solution

Check with your vendors for patches or updates. For information about
a vendor, please see the systems affected section in the individual
vulnerability notes or contact your vendor directly.
Alternatively, apply the appropriate source code patches referenced in
MITKRB5-SA-2007-004 and MITKRB5-SA-2007-005 and recompile.
These vulnerabilities will also be addressed in the krb5-1.6.2 and
krb5-1.5.4 releases.

IV. References

* US-CERT Vulnerability Note VU#365313 - <http://www.kb.cert.org/vuls/id/365313>

* US-CERT Vulnerability Note VU#356961 - <http://www.kb.cert.org/vuls/id/356961>

* US-CERT Vulnerability Note VU#554257 - <http://www.kb.cert.org/vuls/id/554257>

* MIT krb5 Security Advisory 2007-004 -
<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-004.txt>

* MIT krb5 Security Advisory 2007-005 -
<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-005.txt>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/techalerts/TA07-177A.html>

Feedback can be directed to US-CERT Technical Staff. Please send
email to <cert@cert.org> with "TA07-177A Feedback VU#554257" in the
subject.

For instructions on subscribing to or unsubscribing from this
mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Revision History

June 26, 2007: Initial release