

[Full-Disclosure] GLSA: krb5 & mit-krb5 (200303-28)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-03/0288.html>

From: Daniel Ahlberg (aliz@gentoo.org)

Date: 03/31/03

From: Daniel Ahlberg <aliz@gentoo.org>

To: full-disclosure@lists.netsys.com

Date: Mon, 31 Mar 2003 12:01:41 +0200

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

Hash: SHA1

GENTOO LINUX SECURITY ANNOUNCEMENT 200303-28

PACKAGE : krb5 & mit-krb5

SUMMARY : multiple vulnerabilities fixed

DATE : 2003-03-31 10:01 UTC

EXPLOIT : remote

VERSIONS AFFECTED : krb5: <1.2.7-r2 mit-krb5: <1.2.7

FIXED VERSION : krb5: >=1.2.7-r2 mit-krb5: >=1.2.7

CVE : CAN-2003-0139 CAN-2003-0138 CAN-2003-0082

CAN-2003-0072 CAN-2003-0028

- From advisory:

"An attacker who has successfully authenticated to the Kerberos administration daemon (kadmind) may be able to crash kadmind or induce it to leak sensitive information, such as secret keys. For the attack to succeed, it is believed that the configuration of the kadmind installation must allow it to successfully allocate more than INT_MAX bytes of memory."

Read the full advisory at

<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-003-xdr.txt>

- From advisory:

"A cryptographic weakness in version 4 of the Kerberos protocol allows an attacker to use a chosen-plaintext attack to impersonate any principal in a realm. Additional cryptographic weaknesses in the krb4

Full-Disclosure: [Full-Disclosure] GLSA: krb5 & mit-krb5 (200303-28)

implementation included in the MIT krb5 distribution permit the use of
cut-and-paste attacks to fabrica