

MDKSA-2003:021 – Updated krb5 packages fix vulnerability in FTP client

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-02/0252.html>

From: Mandrake Linux Security Team (security@linux-mandrake.com)

Date: 02/21/03

Date: 21 Feb 2003 16:19:00 -0000

From: Mandrake Linux Security Team <security@linux-mandrake.com>

To: bugtraq@securityfocus.com

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

Hash: SHA1

Mandrake Linux Security Update Advisory

Package name: krb5

Advisory ID: MDKSA-2003:021

Date: February 21st, 2003

Affected versions: 8.1, 8.2, 9.0, Multi Network Firewall 8.2

Problem Description:

A vulnerability was discovered in the Kerberos FTP client. When the client retrieves a file that has a filename beginning with a pipe character, the FTP client will pass that filename to the command shell in a system() call. This could allow a malicious remote FTP server to write to files outside of the current directory or even execute arbitrary commands as the user using the FTP client.

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0041>

Updated Packages:

Mandrake Linux 8.1:

2d480884d097bdd03a37e164e92e19fb 8.1/RPMS/ftp-client-krb5-1.2.2-17.4mdk.i586.rpm

SecurityFocus Bugtraq: MDKSA-2003:021 – Updated krb5 packages fix vulnerability in FTP client

79edbe6ae93a0b49c9ebd2bb05c97e50 8.1/RPMS/ftp-server-krb5-1.2.2-17.4mdk.i586.rpm
bf35c3ab6bec9135e4467b8fdad0cc80 8.1/RPMS/krb5-devel-1.2.2-17.4mdk.i586.rpm
ad25706bdaec493ab1eec7f66391195e 8.1/RPMS/krb5-libs-1.2.2-17.4mdk.i586.rpm
af0fa48cfdcff2df3059e54440555868 8.1/RPMS/krb5-server-1.2.2-17.4mdk.i586.rpm
922d81f4beaaad7853e39b0dbbc83fd9 8.1/RPMS/krb5-workstation-1.2.2-17.4mdk.i586.rpm
21b3beae50efac678cf1d313e09b6859 8.1/RPMS/telnet-client-krb5-1.2.2-17.4mdk.i586.rpm
638d0e3a6fb2e6d251fe38758aa623ac 8.1/RPMS/telnet-server-krb5-1.2.2-17.4mdk.i586.rpm
7fce8bd34160b2aadafc04a813a48554 8.1/SRPMS/krb5-1.2.2-17.4mdk.src.rpm

Mandrake Linux 8.1/IA64:

68e7b8b9d8c9f336463f531d07b2f1c9 ia64/8.1/RPMS/ftp-client-krb5-1.2.2-17.4mdk.ia64.rpm
7d3692e7ff1a4e98698ba2153036681b ia64/8.1/RPMS/ftp-server-krb5-1.2.2-17.4mdk.ia64.rpm
b11861cee93afb36e7ee2d55d853e7e8 ia64/8.1/RPMS/krb5-devel-1.2.2-17.4mdk.ia64.rpm
c0fb6cd4ce4e02d8663913b21ddecd6 ia64/8.1/RPMS/krb5-libs-1.2.2-17.4mdk.ia64.rpm
a05cc3b97fc24adfbfac3c780dc29f52 ia64/8.1/RPMS/krb5-server-1.2.2-17.4mdk.ia64.rpm
04e9d98a7eeb7b03ebc704a6efa27f70 ia64/8.1/RPMS/krb5-workstation-1.2.2-17.4mdk.ia64.rpm
34bf6b947272a8851815629267e94d36 ia64/8.1/RPMS/telnet-client-krb5-1.2.2-17.4mdk.ia64.rpm
09a8b6f1f9746edcd8a49f640a8f6caf ia64/8.1/RPMS/telnet-server-krb5-1.2.2-17.4mdk.ia64.rpm
7fce8bd34160b2aadafc04a813a48554 ia64/8.1/SRPMS/krb5-1.2.2-17.4mdk.src.rpm

Mandrake Linux 8.2:

a420e79c59883a7137da026fbeece479 8.2/RPMS/ftp-client-krb5-1.2.2-17.4mdk.i586.rpm
c2e04b717dfa8977afced8908fd00829 8.2/RPMS/ftp-server-krb5-1.2.2-17.4mdk.i586.rpm
f4c35796085b542ccf5984ae6aef3fa3 8.2/RPMS/krb5-devel-1.2.2-17.4mdk.i586.rpm
7b0e5846ba9111e80a0f61b6031c9572 8.2/RPMS/krb5-libs-1.2.2-17.4mdk.i586.rpm
649d509b055b7850e19a800ca4ada374 8.2/RPMS/krb5-server-1.2.2-17.4mdk.i586.rpm
985491105c430433be7fb015d15afb8e 8.2/RPMS/krb5-workstation-1.2.2-17.4mdk.i586.rpm
72bef496f881a48b784a4c9d2684694e 8.2/RPMS/telnet-client-krb5-1.2.2-17.4mdk.i586.rpm
c94980751d86524fdf9a04d4a4d7df88 8.2/RPMS/telnet-server-krb5-1.2.2-17.4mdk.i586.rpm
7fce8bd34160b2aadafc04a813a48554 8.2/SRPMS/krb5-1.2.2-17.4mdk.src.rpm

Mandrake Linux 8.2/PPC:

69cc12b90974facd2211ec445e87ded9 ppc/8.2/RPMS/ftp-client-krb5-1.2.2-17.4mdk.ppc.rpm
de9354b5fae5881e592c2c8a8c2ea110 ppc/8.2/RPMS/ftp-server-krb5-1.2.2-17.4mdk.ppc.rpm
e76f218d156db1bc0c3055be11901f87 ppc/8.2/RPMS/krb5-devel-1.2.2-17.4mdk.ppc.rpm
a2abcd6f614edb2837e8a0b28fc83f9c ppc/8.2/RPMS/krb5-libs-1.2.2-17.4mdk.ppc.rpm
1a4e2ecad97681fad7cddbdeb5dbfddf ppc/8.2/RPMS/krb5-server-1.2.2-17.4mdk.ppc.rpm
4378345e4e5ddaf30db25bbd4c817fb8 ppc/8.2/RPMS/krb5-workstation-1.2.2-17.4mdk.ppc.rpm
3a53dd63aad1582f6f8e97feb1e818 ppc/8.2/RPMS/telnet-client-krb5-1.2.2-17.4mdk.ppc.rpm
a6dc8e41bacd9a5677406aa70347be36 ppc/8.2/RPMS/telnet-server-krb5-1.2.2-17.4mdk.ppc.rpm
7fce8bd34160b2aadafc04a813a48554 ppc/8.2/SRPMS/krb5-1.2.2-17.4mdk.src.rpm

Mandrake Linux 9.0:

43a7c22bca8abdd8565571462799b58d 9.0/RPMS/ftp-client-krb5-1.2.5-1.3mdk.i586.rpm
88c802552ca70467ddbc41d03ffb4a13 9.0/RPMS/ftp-server-krb5-1.2.5-1.3mdk.i586.rpm
f316835b3625c93cb4b7071ef0cdba81 9.0/RPMS/krb5-devel-1.2.5-1.3mdk.i586.rpm
223bcd26f75a053f102edd61b9e32c42 9.0/RPMS/krb5-libs-1.2.5-1.3mdk.i586.rpm
9f47cdc3e0f4e73f2785391401db3606 9.0/RPMS/krb5-server-1.2.5-1.3mdk.i586.rpm
45abe8da8f951dee0085d78c7ba3f48d 9.0/RPMS/krb5-workstation-1.2.5-1.3mdk.i586.rpm
09e43b1a65fe9f7cba15e857b72ab834 9.0/RPMS/telnet-client-krb5-1.2.5-1.3mdk.i586.rpm
e897ba5e26203217039eb56f04796934 9.0/RPMS/telnet-server-krb5-1.2.5-1.3mdk.i586.rpm

SecurityFocus Bugtraq: MDKSA-2003:021 – Updated krb5 packages fix vulnerability in FTP client

e0a9c95f9e66df0b768121b81494c411 9.0/SRPMS/krb5-1.2.5-1.3mdk.src.rpm

Multi Network Firewall 8.2:

7b0e5846ba9111e80a0f61b6031c9572 mnf8.2/RPMS/krb5-libs-1.2.2-17.4mdk.i586.rpm

7fce8bd34160b2aadafc04a813a48554 mnf8.2/SRPMS/krb5-1.2.2-17.4mdk.src.rpm

Bug IDs fixed (see <https://qa.mandrakesoft.com> for more information):

To upgrade automatically, use MandrakeUpdate. The verification of md5 checksums and GPG signatures is performed automatically for you.

If you want to upgrade manually, download the updated package from one of our FTP server mirrors and upgrade with "rpm -Fvh *.rpm". A list of FTP mirrors can be obtained from:

<http://www.mandrakesecure.net/en/ftp.php>

Please verify the update prior to upgrading to ensure the integrity of the downloaded package. You can do this with the command:

```
rpm --checksig <filename>
```

All packages are signed by MandrakeSoft for security. You can obtain the GPG public key of the Mandrake Linux Security Team from:

<https://www.mandrakesecure.net/RPM-GPG-KEYS>

Please be aware that sometimes it takes the mirrors a few hours to update.

You can view other update advisories for Mandrake Linux at:

<http://www.mandrakesecure.net/en/advisories/>

MandrakeSoft has several security-related mailing list services that anyone can subscribe to. Information on these lists can be obtained by visiting:

<http://www.mandrakesecure.net/en/mlist.php>

If you want to report vulnerabilities, please contact

security_linux-mandrake.com

```
Type Bits/KeyID Date User ID  
pub 1024D/22458A98 2000-07-10 Linux Mandrake Security Team  
<security linux-mandrake.com>
```

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.0.7 (GNU/Linux)

mQGIBDlp594RBAC2tDozI3ZgQsE7XwxurJCJrX0L5vx7SDByR5GHDdWekGhdiday
L4nfUax+SeR9SCoCgTgPW1xB8vtQc8/sinJIMjp9197a2iKM0FOcPlkpa3HcOdt7
WKJqQhlMrHvRcsivzcgqjH44GBBJIT6sygUF8k0IU6YnMHj5MPc/NGWt8wCg9vKo
P015QVAFSShtqcU9W8cc7wMEAJzQsAlnvPXDBfBLEH6u7ptWFdp0GvbSuG2wRaPl
hynHvRiE01ZvwbJZXSpsKm1z7uVoW+NknKLunWKB5axrNXDHxCYJBzY3jTeFjsqx
PFZkIEAQphLTkeXXelAjQ5u9tEshPswEtMvJvUgNiAfbzHfPYmq8D6x5xOw1IySg
2e/LBACxr2UJYCCB2BZ3p508mAB0RpuLGukq+7UWiOizy+kSskIBg2O7sQkVY/Cs
iyGEo4XvXqZFMY39RBdfm2GY+WB/5NFiTOYJRKjfrP6K1YbtsmctsX8dG+foKsD
LLFs7OuVfaydLQYp1iiN6D+LJDSMPM8/LCWzZsgr9EKJ8NXiyrQ6TGludXggTWFu
ZHJha2UgU2VjdXJpdHkgVGVhbSA8c2VjdXJpdHlAbGludXgtbWFuZHJha2UuY29t
PohWBBMRAgAWBQI5aefBAsKBAMDFQMCAxYCAQIXgAAKCRCAqNDQIkWKmK6LAKCy
/NInDsaMSI+WHwrquwC5PZrcnQCeI+v3gUDsNfQfiKBvQSANu1hdulqIRgQQEQIA
BgUCOtNVGQAKCRBZ5w3um0pAJJWQAKDUoL5He+mKbfrMaTuyU5lMrYJ0fwCgoFAP
WdvQlu/kFjphF740XeOwtOqIRgQQEQIABgUCOu8A6QAKCRBynDnb9lq3CnpjAJ4w
Pk0SEE9U4r40IxWpwLU+wrWVugCdFfSPllPpZRCiaC7HwbFcfExRmPaIRgQQEQIA
BgUCPI+UAWAKCRDniYrgcHcf8xK5AKCm/Mq8qP8GE0o1hEX22QsJMZwH5gCfZ72H
8TacOb3oAmBdprf+K6gkdOiIRgQQEQIABgUCOtOieAAKCRcv2bZyU0yB80MeAJ9K
+jXt0cKuaUonRU+CRGetk6t9dgCfTRRL6/puOKdD6md70+K5EBBSvsG0OE1hbmRy
YWtlIEExpbnV4IFNIY3VyaXR5IFRIYW0gPHNIY3VyaXR5QG1hbmRyYWtlc29mdC5j
b20+iFcEEExECABcFAjyPnuUFCwcKAwQDFQMCAxYCAQIXgAAKCRCAqNDQIkWKmFi+
AJsHhohgnU3ik4+gy3EdFIB2i/MBoACg6lHn5cnVvTcmgNccWxeNxLLZI5e5AQ0E
OWnn7xAEAQOITVY4TiNo5V/iP0J1xnqjqlqZsU7yEBKo/gZz6/+hx75RURelEbiJ
9F779FQbpJ9Epz1KLSXvq974rnVb813zuGdmgFyk+ryA/rTR2RQ8h+EoNkwmATzR
xBXVJb57fFQjxOu4eNjZAtfII/YXb0uyXXrdr5dIJ/3eXrcO4p0XAAMFBACCxo6Z
269s+A4v8C6Ui12aarOQcCDIV8cVG9LkyatU3FNTlnasqwo6EkaP572448weJWwN
6SCXVI+xOYLik0hL/6Jb/O9Agw75yUVdk+RMM2I4fNEi+y4hmfMh2siBv8yEkEvZ
jTcl3TpkTfzYky85tu433wmKaLFov0WjBFSikohGBBgRAgAGBQI5aefvAAoJEJqo
0NAiRYqYid0AoJgeWzXrEdICIBOSW5Q6FzqJJyaqAKC0Y9YI3UFIE4zSIGjcFILJ
EJGXIA==

=yGIX

-----END PGP PUBLIC KEY BLOCK-----

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

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE+VIFzmjq00CJFipgRAvycAKDBTqx4p0PV3vtcNqtFTiZ3WIHEUgCeL9fr
f4ReAcATO73HSeqq8QJ6p9g=
=n9Ys

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