

[Full-Disclosure] MDKSA-2004:083 – Updated rsync packages fix remotely-exploitable vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/0850.html>

From: Mandrake Linux Security Team (security_at_linux-mandrake.com)

Date: 08/18/04

To: full-disclosure@lists.netsys.com

Date: 17 Aug 2004 22:07:49 -0000

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

Hash: SHA1

Mandrakelinux Security Update Advisory

Package name: rsync

Advisory ID: MDKSA-2004:083

Date: August 17th, 2004

Affected versions: 10.0, 9.1, 9.2, Corporate Server 2.1,
Multi Network Firewall 8.2

Problem Description:

An advisory was sent out by the rsync team regarding a security vulnerability in all versions of rsync prior to and including 2.6.2. If rsync is running in daemon mode, and not in a chrooted environment, it is possible for a remote attacker to trick rsyncd into creating an absolute pathname while sanitizing it. This vulnerability allows a remote attacker to possibly read/write to/from files outside of the rsync directory.

The updated packages are patched to prevent this problem.

References:

http://samba.org/rsync/#security_aug04

Full-Disclosure: [Full-Disclosure] MDKSA-2004:083 – Updated rsync packages fix remotely-exploitable vulnerability

Updated Packages:

Mandrakelinux 10.0:

1b4b64408f1d5db5f4f700de0a4add13 10.0/RPMS/rsync-2.6.0-1.2.100mdk.i586.rpm
094ec110689e485c178adf3310e7e86e 10.0/SRPMS/rsync-2.6.0-1.2.100mdk.src.rpm

Mandrakelinux 10.0/AMD64:

20a09fc79f54be4c14c09bc4bb9652fe amd64/10.0/RPMS/rsync-2.6.0-1.2.100mdk.amd64.rpm
094ec110689e485c178adf3310e7e86e amd64/10.0/SRPMS/rsync-2.6.0-1.2.100mdk.src.rpm

Corporate Server 2.1:

4de66f34494f397f921cb364aeaa162 corporate/2.1/RPMS/rsync-2.5.5-5.3.C21mdk.i586.rpm
61cf910f7e318be0b3b247ce0568b09c corporate/2.1/SRPMS/rsync-2.5.5-5.3.C21mdk.src.rpm

Corporate Server 2.1/x86_64:

0007ae94030d0b6ee773170deb30d867 x86_64/corporate/2.1/RPMS/rsync-2.5.5-5.3.C21mdk.x86_64.rpm
61cf910f7e318be0b3b247ce0568b09c x86_64/corporate/2.1/SRPMS/rsync-2.5.5-5.3.C21mdk.src.rpm

Mandrakelinux 9.1:

98098a144b62ed85da5778b63293f614 9.1/RPMS/rsync-2.5.7-0.3.91mdk.i586.rpm
088606d2269e99f9f8dd99c095744ec3 9.1/SRPMS/rsync-2.5.7-0.3.91mdk.src.rpm

Mandrakelinux 9.1/PPC:

8f5cc0a974b614bbe63ac01445c54ac3 ppc/9.1/RPMS/rsync-2.5.7-0.3.91mdk.ppc.rpm
088606d2269e99f9f8dd99c095744ec3 ppc/9.1/SRPMS/rsync-2.5.7-0.3.91mdk.src.rpm

Mandrakelinux 9.2:

1fef094e97d7c40a2892167e19605dc3 9.2/RPMS/rsync-2.5.7-0.3.92mdk.i586.rpm
b98e8c0684ab6dd8b9f30b45de076e95 9.2/SRPMS/rsync-2.5.7-0.3.92mdk.src.rpm

Mandrakelinux 9.2/AMD64:

06e06a5c39ecdeec4780c7026041f339 amd64/9.2/RPMS/rsync-2.5.7-0.3.92mdk.amd64.rpm
b98e8c0684ab6dd8b9f30b45de076e95 amd64/9.2/SRPMS/rsync-2.5.7-0.3.92mdk.src.rpm

Multi Network Firewall 8.2:

b2cd2101e8900eb64b8a4fe0cf527c7e mnf8.2/RPMS/rsync-2.5.4-2.3.M82mdk.i586.rpm
9bf7b6090f06886ca50715127ae06618 mnf8.2/SRPMS/rsync-2.5.4-2.3.M82mdk.src.rpm

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

All packages are signed by Mandrakesoft for security. You can obtain the GPG public key of the Mandrakelinux Security Team by executing:

```
gpg --recv-keys --keyserver pgp.mit.edu 0x22458A98
```

You can view other update advisories for Mandrakelinux at:

<http://www.mandrakesoft.com/security/advisories>

Full-Disclosure: [Full-Disclosure] MDKSA-2004:083 – Updated rsync packages fix remotely-exploitable vulnerabilities

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 SIGNATURE-----

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQFBIoG1mqjQ0CJFipgRAnmBAJ9OXVMq/9phOtdB9P/dlaZuU7XPGQCglzEx

CSc/YTVSIZOJT7tytctylg=

=v4pW

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

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>