RSYNC exploit: A path-sanitizing bug may allow an attacker to read and write files outside the rsync directory.

RSYNC exploit: A path-sanitizing bug may allow an attacker to read and write files outside the rsync directory. 2003-08-16, LinuxReviews.org

The bug is only present when rsync is running in daemon-mode and without a chroot environment. Most Linux distributions, like Suse and Gentoo, have use chroot = true default settings.

SUSE Linux made updated rsync packages available 2004-08-16, two days after Gentoo Linux. The updates fix a path-sanitizing bug described in a official rsync security advisory 2004-08-12.

The SUSE advisory warn they have yet to release updates packages to fix known security problems with KDE, mozilla/firefox, xine-lib, opera and acroread.

The discovered rsync bug is quite serious, as it allows attackers to read and write outside the intended rsync directory. This can only happen when rsync is running in daemon mode with chroot mode off. You should make sure you are using chroot = true, there is never ever a good reason to turn this feature off. This is why SUSE, Gentoo and other Linux distributions enable the use of a chroot environment by default.

- rsync homepage (samba.org)
- manual page of chroot
- manual page of rsync
RSYNC exploit: A path-sanitizing bug may allow an attacker to read and write files outside the rsync directory.