

NAME

smrsh - restricted shell for sendmail

SYNOPSIS

smrsh -c command

DESCRIPTION

The *smrsh* program is intended as a replacement for *sh* for use in the “prog” mailer in *sendmail*(8) configuration files. It sharply limits the commands that can be run using the “[program]” syntax of *sendmail* in order to improve the over all security of your system. Briefly, even if a “bad guy” can get sendmail to run a program without going through an alias or forward file, *smrsh* limits the set of programs that he or she can execute.

Briefly, *smrsh* limits programs to be in a single directory, by default /usr/libexec/sm.bin, allowing the system administrator to choose the set of acceptable commands, and to the shell builtin commands “exec”, “exit”, and “echo”. It also rejects any commands with the characters “”, “<”, “>”, “;”, “\$”, “(”, “)”, “\r” (carriage return), or “\n” (newline) on the command line to prevent “end run” attacks. It allows “||” and “&&” to enable commands like: “|exec /usr/local/bin/filter || exit 75”

Initial pathnames on programs are stripped, so forwarding to “/usr/bin/vacation”, “/home/server/mydir/bin/vacation”, and “vacation” all actually forward to “/usr/libexec/sm.bin/vacation”.

System administrators should be conservative about populating the sm.bin directory. For example, a reasonable additions is *vacation*(1), and the like. No matter how brow-beaten you may be, never include any shell or shell-like program (such as *perl*(1)) in the sm.bin directory. Note that this does not restrict the use of shell or perl scripts in the sm.bin directory (using the “#!” syntax); it simply disallows execution of arbitrary programs. Also, including mail filtering programs such as *procmail*(1) is a very bad idea. *procmail*(1) allows users to run arbitrary programs in their *procmailrc*(5).

COMPILATION

Compilation should be trivial on most systems. You may need to use -DSMRSH_PATH=“*path*” to adjust the default search path (defaults to “/bin:/usr/bin”) and/or -DSMRSH_CMDDIR=“*dir*” to change the default program directory (defaults to “/usr/libexec/sm.bin”).

FILES

/usr/adm/sm.bin - default directory for restricted programs on most OSs

/var/adm/sm.bin - directory for restricted programs on HP UX and Solaris

/usr/libexec/sm.bin - directory for restricted programs on FreeBSD (≥ 3.3) and DragonFly BSD

SEE ALSO

sendmail(8)