

## 5.X Tripwire Policy File

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-09/0046.html>

---

**From:** Bret Walker (*bret-walker\_at\_northwestern.edu*)

**Date:** 09/28/05

Date: Tue, 27 Sep 2005 19:30:14 -0500

To: freebsd-security <freebsd-security@freebsd.org>

Hello all.

I am just setting up my first 5.X box, and I'm in the process of fine tuning my tripwire policy file.

I am much more familiar with 4.X than I am with 5, so I'm worried that I may be missing a critical element of 5.X in my policy file. Cy (the tripwire port maintainer) updated the policy file to a certain extent, but I would appreciate it if those on the security list would provide some more feedback as to what should definitely be in a tripwire policy file for a 5.X box.

I know most good sysadmins use tripwire, so I think it would be good to have a well thought out policy file for 5.X that others may use as well.

I've attached mine to this message.

Thanks,

Bret

```
#  
# Policy file for FreeBSD  
#  
# $FreeBSD: ports/security/tripwire/files/twpol.txt,v 1.3 2005/08/09 18:24:15 cy Exp $
```

```
#  
# This is the example Tripwire Policy file. It is intended as a place to  
# start creating your own custom Tripwire Policy file. Referring to it as  
# well as the Tripwire Policy Guide should give you enough information to  
# make a good custom Tripwire Policy file that better covers your  
# configuration and security needs. A text version of this policy file is  
# called twpol.txt.  
#
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
# Note that this file is tuned to an install of FreeBSD using
# buildworld. If run unmodified, this file should create no errors on
# database creation, or violations on a subsequent integrity check.
# However it is impossible for there to be one policy file for all machines,
# so this existing one errs on the side of security. Your FreeBSD
# configuration will most likely differ from the one our policy file was
# tuned to, and will therefore require some editing of the default
# Tripwire Policy file.
#
# The example policy file is best run with 'Loose Directory Checking'
# enabled. Set LOOSEDIRECTORYCHECKING=TRUE in the Tripwire Configuration
# file.
#
# Email support is not included and must be added to this file.
# Add the 'mailto=' to the rule directive section of each rule (add a comma
# after the 'severity=' line and add an 'mailto=' and include the email
# addresses you want the violation reports to go to). Addresses are
# semi-colon delimited.
#
#
# Global Variable Definitions
#
# These are defined at install time by the installation script. You may
# Manually edit these if you are using this file directly and not from the
# installation script itself.
#
@@section GLOBAL
TWDOCS="/usr/local/share/doc/tripwire";
TWBIN="/usr/local/sbin";
TWPOL="/usr/local/etc/tripwire";
TWDB="/var/db/tripwire";
TWSKEY="/usr/local/etc/tripwire";
TWLKEY="/usr/local/etc/tripwire";
TWREPORT="/var/db/tripwire/report";
HOSTNAME=speedy.medill.northwestern.edu;

@@section FS
SEC_CRIT = $(IgnoreNone)-SHa ; # Critical files that cannot change
SEC_SUID = $(IgnoreNone)-SHa ; # Binaries with the SUID or SGID flags set
SEC_BIN = $(ReadOnly) ; # Binaries that should not change
SEC_CONFIG = $(Dynamic) ; # Config files that are changed infrequently but accessed often
SEC_TTY = $(Dynamic)-ugp ; # Tty files that change ownership at login
SEC_LOG = $(Growing) ; # Files that grow, but that should never change ownership
SEC_INVARIANT = +tpug ; # Directories that should never change permission or ownership
SIG_LOW = 33 ; # Non-critical files that are of minimal security impact
SIG_MED = 66 ; # Non-critical files that are of significant security impact
SIG_HI = 100 ; # Critical files that are significant points of vulnerability
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen -> $(SEC_BIN) ;
  $(TWBIN)/tripwire -> $(SEC_BIN) ;
  $(TWBIN)/twadmin -> $(SEC_BIN) ;
  $(TWBIN)/twprint -> $(SEC_BIN) ;
}

# Tripwire Data Files – Configuration Files, Policy Files, Keys, Reports, Databases
(
  rulename = "Tripwire Data Files",
  severity = $(SIG_HI)
)
{
  # NOTE: We remove the inode attribute because when Tripwire creates a backup,
  # it does so by renaming the old file and creating a new one (which will
  # have a new inode number). Inode is left turned on for keys, which shouldn't
  # ever change.

  # NOTE: The first integrity check triggers this rule and each integrity check
  # afterward triggers this rule until a database update is run, since the
  # database file does not exist before that point.

  $(TWDB) -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg -> $(SEC_BIN) -i ;
  $(TWPOL)/twcfg.txt -> $(SEC_BIN) ;
  $(TWPOL)/twpol.txt -> $(SEC_BIN) ;
  $(TWLKEY)/$(HOSTNAME)-local.key -> $(SEC_BIN) ;
  $(TWSKEY)/site.key -> $(SEC_BIN) ;

  #don't scan the individual reports
  $(TWREPORT) -> $(SEC_CONFIG) (recurse=0) ;
}

# Tripwire HQ Connector Binaries
#(
#  # rulename = "Tripwire HQ Connector Binaries",
#  # severity = $(SIG_HI)
#)
#{
#  # $(TWBIN)/hqagent -> $(SEC_BIN) ;
#}
#
# Tripwire HQ Connector – Configuration Files, Keys, and Logs
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
#
# Note: File locations here are different than in a stock HQ Connector
# installation. This is because Tripwire 2.3 uses a different path
# structure than Tripwire 2.2.1.
#
# You may need to update your HQ Agent configuration file (or this policy
# file) to correct the paths. We have attempted to support the FHS standard
# here by placing the HQ Agent files similarly to the way Tripwire 2.3
# places them.
#

#(
# rulename = "Tripwire HQ Connector Data Files",
# severity = $(SIG_HI)
#)
#{
#
# # NOTE: Removing the inode attribute because when Tripwire creates a backup
# # it does so by renaming the old file and creating a new one (which will
# # have a new inode number). Leaving inode turned on for keys, which
# # shouldn't ever change.
#
#
# $(TWBIN)/agent.cfg -> $(SEC_BIN) -i ;
# $(TWLKEY)/authentication.key -> $(SEC_BIN) ;
# $(TWDB)/tasks.dat -> $(SEC_CONFIG) ;
# $(TWDB)/schedule.dat -> $(SEC_CONFIG) ;
#
# # Uncomment if you have agent logging enabled.
# #/var/log/tripwire/agent.log -> $(SEC_LOG) ;
#}

# Commonly accessed directories that should remain static with regards to owner and group
(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)
{
  / -> $(SEC_INVARIANT) (recurse = false) ;
  /home -> $(SEC_INVARIANT) (recurse = false) ;
}

#
# First, root's "home"
#

(
  rulename = "Root's home",
  severity = $(SIG_HI)
)
{
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
# /.rhosts -> $(SEC_CRIT) ;
/.profile -> $(SEC_CRIT) ;
/.cshrc -> $(SEC_CRIT) ;
# /.login -> $(SEC_CRIT) ;
# /.exrc -> $(SEC_CRIT) ;
# /.logout -> $(SEC_CRIT) ;
# /.forward -> $(SEC_CRIT) ;
/root -> $(SEC_CRIT) (recurse = true) ;
!/root/.history ;
!/root/.bash_history ;
# !/root/.lsof_SYSTEM_NAME ; # Uncomment if lsof is installed
}

#
# FreeBSD Kernel
#

(
  rulename = "FreeBSD Kernel",
  severity = $(SIG_HI)
)
{
  # /boot is used by FreeBSD 5.X+
  /boot -> $(SEC_CRIT) ;
  # /kernel is used by FreeBSD 4.X
  # /kernel -> $(SEC_CRIT) ;
  # /kernel.old -> $(SEC_CRIT) ;
  # /kernel.GENERIC -> $(SEC_CRIT) ;
}

#
# FreeBSD Modules
#

(
  rulename = "FreeBSD Modules",
  severity = $(SIG_HI)
)
{
  # /modules is used by FreeBSD 4.X
  # /modules -> $(SEC_CRIT) (recurse = true) ;
  # /modules.old -> $(SEC_CRIT) (recurse = true) ;
  # /lkm is used by FreeBSD 2.X and 3.X
  # /lkm -> $(SEC_CRIT) (recurse = true) ; # uncomment if using lkm kld
}

#
# System Administration Programs
#
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
(
  rulename = "System Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin -> $(SEC_CRIT) (recurse = true) ;
  /usr/sbin -> $(SEC_CRIT) (recurse = true) ;
}

#
# User Utilities
#

(
  rulename = "User Utilities",
  severity = $(SIG_HI)
)
{
  /bin -> $(SEC_CRIT) (recurse = true) ;
  /usr/bin -> $(SEC_CRIT) (recurse = true) ;
}

#
# /dev
#

(
  rulename = "/dev",
  severity = $(SIG_HI)
)
{
  # XXX Do we really need to verify the integrity of /dev on 5.X?
  # /dev -> $(Device) (recurse = true) ;
  # !/dev/vga ;
  # !/dev/dri ;
  # /dev/console -> $(SEC_TTY) ;
  # /dev/ttyv0 -> $(SEC_TTY) ;
  # /dev/ttyv1 -> $(SEC_TTY) ;
  # /dev/ttyv2 -> $(SEC_TTY) ;
  # /dev/ttyv3 -> $(SEC_TTY) ;
  # /dev/ttyv4 -> $(SEC_TTY) ;
  # /dev/ttyv5 -> $(SEC_TTY) ;
  # /dev/ttyv6 -> $(SEC_TTY) ;
  # /dev/ttyv7 -> $(SEC_TTY) ;
  # /dev/typ0 -> $(SEC_TTY) ;
  # /dev/typ1 -> $(SEC_TTY) ;
  # /dev/typ2 -> $(SEC_TTY) ;
  # /dev/typ3 -> $(SEC_TTY) ;
  # /dev/typ4 -> $(SEC_TTY) ;
  # /dev/typ5 -> $(SEC_TTY) ;
  # /dev/typ6 -> $(SEC_TTY) ;
}
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
# /dev/tty7 -> $(SEC_TTY) ;
# /dev/tty8 -> $(SEC_TTY) ;
# /dev/tty9 -> $(SEC_TTY) ;
# /dev/ttya -> $(SEC_TTY) ;
# /dev/ttyb -> $(SEC_TTY) ;
# /dev/ttyc -> $(SEC_TTY) ;
# /dev/ttyd -> $(SEC_TTY) ;
# /dev/ttye -> $(SEC_TTY) ;
# /dev/ttyf -> $(SEC_TTY) ;
# /dev/ttyg -> $(SEC_TTY) ;
# /dev/ttyh -> $(SEC_TTY) ;
# /dev/ttyi -> $(SEC_TTY) ;
# /dev/ttyj -> $(SEC_TTY) ;
# /dev/ttyk -> $(SEC_TTY) ;
# /dev/ttyl -> $(SEC_TTY) ;
# /dev/ttym -> $(SEC_TTY) ;
# /dev/ttyn -> $(SEC_TTY) ;
# /dev/ttyo -> $(SEC_TTY) ;
# /dev/ttyp -> $(SEC_TTY) ;
# /dev/ttyq -> $(SEC_TTY) ;
# /dev/ttyr -> $(SEC_TTY) ;
# /dev/ttyt -> $(SEC_TTY) ;
# /dev/ttyu -> $(SEC_TTY) ;
# /dev/ttyv -> $(SEC_TTY) ;
# /dev/cuaa0 -> $(SEC_TTY) ; # modem
}

#
# /etc
#

(
  rulename = "/etc",
  severity = $(SIG_HI)
)
{
  /etc -> $(SEC_CRIT) (recurse = true) ;
  # /etc/mail/aliases -> $(SEC_CONFIG) ;
  /etc/dumpdates -> $(SEC_CONFIG) ;
  /etc/motd -> $(SEC_CONFIG) ;
  !/etc/ppp/connect-errors ;
# /etc/skeykeys -> $(SEC_CONFIG) ;
# Uncomment the following 4 lines if your password file does not change
# /etc/passwd -> $(SEC_CONFIG) ;
# /etc/master.passwd -> $(SEC_CONFIG) ;
# /etc/pwd.db -> $(SEC_CONFIG) ;
# /etc/spwd.db -> $(SEC_CONFIG) ;
}

#
# Copatibility (Linux)
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
#  
  
(  
  rulename = "Linux Compatibility",  
  severity = $(SIG_HI)  
)  
{  
  /compat -> $(SEC_CRIT) (recurse = true) ;  
#  
# Uncomment the following if Linux compatibility is used. Replace  
# HOSTNAME1 and HOSTNAME2 with the hosts that have Linux emulation port  
# installed.  
#  
#@@ifhost HOSTNAME1 || HOSTNAME2  
# /compat/linux/etc -> $(SEC_INVARIANT) (recurse = false) ;  
# /compat/linux/etc/X11 -> $(SEC_CONFIG) (recurse = true) ;  
# /compat/linux/etc/pam.d -> $(SEC_CONFIG) (recurse = true) ;  
# /compat/linux/etc/profile.d -> $(SEC_CONFIG) (recurse = true) ;  
# /compat/linux/etc/real -> $(SEC_CONFIG) (recurse = true) ;  
# /compat/linux/etc/bashrc -> $(SEC_CONFIG) ;  
# /compat/linux/etc/csh.login -> $(SEC_CONFIG) ;  
# /compat/linux/etc/host.conf -> $(SEC_CONFIG) ;  
# /compat/linux/etc/hosts.allow -> $(SEC_CONFIG) ;  
# /compat/linux/etc/hosts.deny -> $(SEC_CONFIG) ;  
# /compat/linux/etc/info-dir -> $(SEC_CONFIG) ;  
# /compat/linux/etc/inputrc -> $(SEC_CONFIG) ;  
# /compat/linux/etc/ld.so.conf -> $(SEC_CONFIG) ;  
# /compat/linux/etc/nsswitch.conf -> $(SEC_CONFIG) ;  
# /compat/linux/etc/profile -> $(SEC_CONFIG) ;  
# /compat/linux/etc/redhat-release -> $(SEC_CONFIG) ;  
# /compat/linux/etc/rpc -> $(SEC_CONFIG) ;  
# /compat/linux/etc/securetty -> $(SEC_CONFIG) ;  
# /compat/linux/etc/shells -> $(SEC_CONFIG) ;  
# /compat/linux/etc/termcap -> $(SEC_CONFIG) ;  
# /compat/linux/etc/yp.conf -> $(SEC_CONFIG) ;  
# !/compat/linux/etc/ld.so.cache ;  
# !/compat/linux/var/spool/mail ;  
#@@endif  
}  
  
#  
# Libraries, include files, and other system files  
#  
  
(  
  rulename = "Libraries, include files, and other system files",  
  severity = $(SIG_HI)  
)  
{  
  /usr/include -> $(SEC_CRIT) (recurse = true) ;  
  /usr/lib -> $(SEC_CRIT) (recurse = true) ;
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
/usr/libdata -> $(SEC_CRIT) (recurse = true) ;
/usr/libexec -> $(SEC_CRIT) (recurse = true) ;
/usr/share -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man -> $(SEC_CONFIG) ;
!usr/share/man/whatis ;
!usr/share/man/.glimpse_filenames ;
!usr/share/man/.glimpse_filenames_index ;
!usr/share/man/.glimpse_filetimes ;
!usr/share/man/.glimpse_filters ;
!usr/share/man/.glimpse_index ;
!usr/share/man/.glimpse_messages ;
!usr/share/man/.glimpse_partitions ;
!usr/share/man/.glimpse_statistics ;
!usr/share/man/.glimpse_turbo ;
/usr/share/man/man1 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man2 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man3 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man4 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man5 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man6 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man7 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man8 -> $(SEC_CRIT) (recurse = true) ;
/usr/share/man/man9 -> $(SEC_CRIT) (recurse = true) ;
# /usr/share/man/mann -> $(SEC_CRIT) (recurse = true) ;
! /usr/share/man/cat1 ;
! /usr/share/man/cat2 ;
! /usr/share/man/cat3 ;
! /usr/share/man/cat4 ;
! /usr/share/man/cat5 ;
! /usr/share/man/cat6 ;
! /usr/share/man/cat7 ;
! /usr/share/man/cat8 ;
! /usr/share/man/cat9 ;
! /usr/share/man/catl ;
! /usr/share/man/catn ;
# /usr/share/perl/man -> $(SEC_CONFIG) ;
!usr/share/perl/man/whatis ;
!usr/share/perl/man/.glimpse_filenames ;
!usr/share/perl/man/.glimpse_filenames_index ;
!usr/share/perl/man/.glimpse_filetimes ;
!usr/share/perl/man/.glimpse_filters ;
!usr/share/perl/man/.glimpse_index ;
!usr/share/perl/man/.glimpse_messages ;
!usr/share/perl/man/.glimpse_partitions ;
!usr/share/perl/man/.glimpse_statistics ;
!usr/share/perl/man/.glimpse_turbo ;
# /usr/share/perl/man/man3 -> $(SEC_CRIT) (recurse = true) ;
! /usr/share/perl/man/cat3 ;
# /usr/local/lib/perl5/5.00503/man -> $(SEC_CONFIG) ;
! /usr/local/lib/perl5/5.00503/man/whatis ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_filters ;
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
! /usr/local/lib/perl5/5.00503/man/.glimpse_filetimes ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_messages ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_statistics ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_index ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_turbo ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_partitions ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_filenames ;
! /usr/local/lib/perl5/5.00503/man/.glimpse_filenames_index ;
# /usr/local/lib/perl5/5.00503/man/man3 -> $(SEC_CRIT) (recurse = true) ;
! /usr/local/lib/perl5/5.00503/man/cat3 ;
}

#
# X11R6
#

(
  rulename = "X11R6",
  severity = $(SIG_HI)
)
{
  /usr/X11R6 -> $(SEC_CRIT) (recurse = true) ;
# /usr/X11R6/lib/X11/xdm -> $(SEC_CONFIG) (recurse = true) ;
! /usr/X11R6/lib/X11/xdm/xdm-errors ;
! /usr/X11R6/lib/X11/xdm/authdir/authfiles ;
! /usr/X11R6/lib/X11/xdm/xdm-pid ;
# /usr/X11R6/lib/X11/xkb/compiled -> $(SEC_CONFIG) (recurse = true) ;
! /usr/X11R6/man -> $(SEC_CONFIG) ;
! /usr/X11R6/man/whatis ;
! /usr/X11R6/man/.glimpse_filenames ;
! /usr/X11R6/man/.glimpse_filenames_index ;
! /usr/X11R6/man/.glimpse_filetimes ;
! /usr/X11R6/man/.glimpse_filters ;
! /usr/X11R6/man/.glimpse_index ;
! /usr/X11R6/man/.glimpse_messages ;
! /usr/X11R6/man/.glimpse_partitions ;
! /usr/X11R6/man/.glimpse_statistics ;
! /usr/X11R6/man/.glimpse_turbo ;
! /usr/X11R6/man/man1 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man2 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man3 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man4 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man5 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man6 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man7 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man8 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/man9 -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/manl -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/mann -> $(SEC_CRIT) (recurse = true) ;
! /usr/X11R6/man/cat1 ;
! /usr/X11R6/man/cat2 ;
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
! /usr/X11R6/man/cat3 ;
! /usr/X11R6/man/cat4 ;
! /usr/X11R6/man/cat5 ;
! /usr/X11R6/man/cat6 ;
! /usr/X11R6/man/cat7 ;
! /usr/X11R6/man/cat8 ;
! /usr/X11R6/man/cat9 ;
! /usr/X11R6/man/cat1 ;
! /usr/X11R6/man/catn ;
}

#
# sources
#

(
  rulename = "Sources",
  severity = $(SIG_HI)
)
{
  /usr/src -> $(SEC_CRIT) (recurse = true) ;
# /usr/src/sys/compile -> $(SEC_CONFIG) (recurse = false) ;
}

#
# NIS
#

(
  rulename = "NIS",
  severity = $(SIG_HI)
)
{
  /var/yp -> $(SEC_CRIT) (recurse = true) ;
  !/var/yp/binding ;
}

#
# Temporary directories
#

(
  rulename = "Temporary directories",
  recurse = false,
  severity = $(SIG_LOW)
)
{
# /usr/tmp -> $(SEC_INVARIANT) ;
  /var/tmp -> $(SEC_INVARIANT) ;
  /var/preserve -> $(SEC_INVARIANT) ;
  /tmp -> $(SEC_INVARIANT) ;
}


```

## FreeBSD–Security: 5.X Tripwire Policy File

```
#
# Local files
#

(
  rulename = "Local files",
  severity = $(SIG_MED)
)
{
  /usr/local/bin -> $(SEC_BIN) (recurse = true) ;
  /usr/local/sbin -> $(SEC_BIN) (recurse = true) ;
  /usr/local/etc -> $(SEC_BIN) (recurse = true) ;
  /usr/local/lib -> $(SEC_BIN) (recurse = true) ;
  /usr/local/libexec -> $(SEC_BIN) (recurse = true) ;
  /usr/local/share -> $(SEC_BIN) (recurse = true) ;
  /usr/local/man -> $(SEC_CONFIG) ;
  !/usr/local/man/whatis ;
  !/usr/local/man/.glimpse_filenames ;
  !/usr/local/man/.glimpse_filenames_index ;
  !/usr/local/man/.glimpse_filetimes ;
  !/usr/local/man/.glimpse_filters ;
  !/usr/local/man/.glimpse_index ;
  !/usr/local/man/.glimpse_messages ;
  !/usr/local/man/.glimpse_partitions ;
  !/usr/local/man/.glimpse_statistics ;
  !/usr/local/man/.glimpse_turbo ;
  /usr/local/man/man1 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man2 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man3 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man4 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man5 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man6 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man7 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man8 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/man9 -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/manl -> $(SEC_CRIT) (recurse = true) ;
  /usr/local/man/mann -> $(SEC_CRIT) (recurse = true) ;
  ! /usr/local/man/cat1 ;
  ! /usr/local/man/cat2 ;
  ! /usr/local/man/cat3 ;
  ! /usr/local/man/cat4 ;
  ! /usr/local/man/cat5 ;
  ! /usr/local/man/cat6 ;
  ! /usr/local/man/cat7 ;
  ! /usr/local/man/cat8 ;
  ! /usr/local/man/cat9 ;
  ! /usr/local/man/catl ;
  ! /usr/local/man/catn ;
  # /usr/local/krb5 -> $(SEC_CRIT) (recurse = true) ;
  # /usr/local/krb5/man -> $(SEC_CONFIG) ;
  !/usr/local/krb5/man/whatis ;
}
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
!/usr/local/krb5/man/.glimpse_filenames ;
!/usr/local/krb5/man/.glimpse_filenames_index ;
!/usr/local/krb5/man/.glimpse_filetimes ;
!/usr/local/krb5/man/.glimpse_filters ;
!/usr/local/krb5/man/.glimpse_index ;
!/usr/local/krb5/man/.glimpse_messages ;
!/usr/local/krb5/man/.glimpse_partitions ;
!/usr/local/krb5/man/.glimpse_statistics ;
!/usr/local/krb5/man/.glimpse_turbo ;
# /usr/local/krb5/man/man1 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man2 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man3 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man4 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man5 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man6 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man7 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man8 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/man9 -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/manl -> $(SEC_CRIT) (recurse = true) ;
# /usr/local/krb5/man/mann -> $(SEC_CRIT) (recurse = true) ;
! /usr/local/krb5/man/cat1 ;
! /usr/local/krb5/man/cat2 ;
! /usr/local/krb5/man/cat3 ;
! /usr/local/krb5/man/cat4 ;
! /usr/local/krb5/man/cat5 ;
! /usr/local/krb5/man/cat6 ;
! /usr/local/krb5/man/cat7 ;
! /usr/local/krb5/man/cat8 ;
! /usr/local/krb5/man/cat9 ;
! /usr/local/krb5/man/catl ;
! /usr/local/krb5/man/catn ;
/usr/local/www -> $(SEC_CONFIG) (recurse = true) ;
}

(
  rulename = "Security Control",
  severity = $(SIG_HI)
)
{
  /etc/group -> $(SEC_CRIT) ;
  /etc/crontab -> $(SEC_CRIT) ;
}

#=====
#
# Copyright 2000 Tripwire, Inc. Tripwire is a registered trademark of Tripwire,
# Inc. in the United States and other countries. All rights reserved.
#
# FreeBSD is a registered trademark of the FreeBSD Project Inc.
#
# UNIX is a registered trademark of The Open Group.
```

## FreeBSD–Security: 5.X Tripwire Policy File

```
#
#=====
#
# Permission is granted to make and distribute verbatim copies of this document
# provided the copyright notice and this permission notice are preserved on all
# copies.
#
# Permission is granted to copy and distribute modified versions of this
# document under the conditions for verbatim copying, provided that the entire
# resulting derived work is distributed under the terms of a permission notice
# identical to this one.
#
# Permission is granted to copy and distribute translations of this document
# into another language, under the above conditions for modified versions,
# except that this permission notice may be stated in a translation approved by
# Tripwire, Inc.
#
# DCM
```

---

- application/x-pkcs7-signature attachment: [S/MIME Cryptographic Signature](#)