NAME

mac_seeotheruids - simple policy controlling whether users see other users

SYNOPSIS

To compile the policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_SEEOTHERUIDS
```

Alternately, to load the module at boot time, place the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5):

```
mac_seeotheruids_load="YES"
```

DESCRIPTION

The **mac_seeotheruids** policy module, when enabled, denies users to see processes or sockets owned by other users.

To enable **mac_seeotheruids**, set the sysctl OID *security.mac.seeotheruids.enabled* to 1. To permit superuser awareness of other credentials by virtue of privilege, set the sysctl OID *security.mac.seeotheruids.suser_privileged* to 1.

To allow users to see processes and sockets owned by the same primary group, set the sysctl OID *security.mac.seeotheruids.primarygroup_enabled* to 1.

To allow processes with a specific group ID to be exempt from the policy, set the sysctl OID *security.mac.seeotheruids.specificgid_enabled* to 1, and *security.mac.seeotheruids.specificgid* to the group ID to be exempted.

Label Format

No labels are defined for **mac_seeotheruids**.

SEE ALSO

mac(4), mac_biba(4), mac_bsdextended(4), mac_ddb(4), mac_ifoff(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_partition(4), mac_portacl(4), mac_test(4), mac(9)

HISTORY

The **mac_seeotheruids** policy module first appeared in FreeBSD 5.0 and was developed by the TrustedBSD Project.

AUTHORS

This software was contributed to the FreeBSD Project by Network Associates Labs, the Security Research Division of Network Associates Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

BUGS

While the MAC Framework design is intended to support the containment of the root user, not all attack channels are currently protected by entry point checks. As such, MAC Framework policies should not be relied on, in isolation, to protect against a malicious privileged user.