

[patch 024/198] SELinux: add support for NETLINK_KOBJECT_UEVENT

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-04/3645.html>

akpm_at_osdl.org

Date: 04/12/05

To: torvalds@osdl.org

Date: Tue, 12 Apr 2005 03:30:54 -0700

From: James Morris <jmorris@redhat.com>

This patch adds SELinux support for the KOBJECT_UEVENT Netlink family, so that SELinux can apply finer grained controls to it. For example, security policy for hald can be locked down to the KOBJECT_UEVENT Netlink family only. Currently, this family simply defaults to the default Netlink socket class.

Note that some new permission definitions are added to sync with changes in the core userspace policy package, which auto-generates header files.

Signed-off-by: James Morris <jmorris@redhat.com>

Signed-off-by: Stephen Smalley <sds@tycho.nsa.gov>

Signed-off-by: Andrew Morton <akpm@osdl.org>

```
25-akpm/security/selinux/hooks.c | 2 +
25-akpm/security/selinux/include/av_inherit.h | 1
25-akpm/security/selinux/include/av_perm_to_string.h | 4 ++
25-akpm/security/selinux/include/av_permissions.h | 28 ++++++
25-akpm/security/selinux/include/class_to_string.h | 2 +
25-akpm/security/selinux/include/flask.h | 2 +
6 files changed, 39 insertions(+)
```

```
diff -puN security/selinux/hooks.c~selinux-add-support-for-netlink_kobject_uevent security/selinux
```

```
--- 25/security/selinux/hooks.c~selinux-add-support-for-netlink_kobject_uevent 2005-04-12 03:21:
```

```
+++ 25-akpm/security/selinux/hooks.c 2005-04-12 03:21:09.243731640 -0700
```

```
@@ -672,6 +672,8 @@ static inline u16 socket_type_to_securit
        return SECCLASS_NETLINK_IP6FW_SOCKET;
    case NETLINK_DNRTMSG:
        return SECCLASS_NETLINK_DNRT_SOCKET;
+   case NETLINK_KOBJECT_UEVENT:
+       return SECCLASS_NETLINK_KOBJECT_UEVENT_SOCKET;
    default:
        return SECCLASS_NETLINK_SOCKET;
}
```

```
diff -puN security/selinux/include/av_inherit.h~selinux-add-support-for-netlink_kobject_uevent se
```

```
--- 25/security/selinux/include/av_inherit.h~selinux-add-support-for-netlink_kobject_uevent 2
```

```
+++ 25-akpm/security/selinux/include/av_inherit.h 2005-04-12 03:21:09.243731640 -0700
```

```
@@ -28,3 +28,4 @@
```

Linux-Kernel: [patch 024/198] SELinux: add support for NETLINK_KOBJECT_UEVENT

```
S_(SECCLASS_NETLINK_AUDIT_SOCKET, socket, 0x00400000UL)
S_(SECCLASS_NETLINK_IP6FW_SOCKET, socket, 0x00400000UL)
S_(SECCLASS_NETLINK_DNRT_SOCKET, socket, 0x00400000UL)
+ S_(SECCLASS_NETLINK_KOBJECT_UEVENT_SOCKET, socket, 0x00400000UL)
diff -puN security/selinux/include/av_permissions.h~selinux-add-support-for-netlink_kobject_ueven
--- 25/security/selinux/include/av_permissions.h~selinux-add-support-for-netlink_kobject_uevent 2
+++ 25-akpm/security/selinux/include/av_permissions.h 2005-04-12 03:21:09.245731336 -0700
@@ -559,6 +559,8 @@
 #define CAPABILITY__SYS_TTY_CONFIG 0x04000000UL
 #define CAPABILITY__MKNOD 0x08000000UL
 #define CAPABILITY__LEASE 0x10000000UL
+#define CAPABILITY__AUDIT_WRITE 0x20000000UL
+#define CAPABILITY__AUDIT_CONTROL 0x40000000UL

 #define PASSWD__PASSWD 0x00000001UL
 #define PASSWD__CHFN 0x00000002UL
@@ -900,3 +902,29 @@
 #define NSCD__SHMEMGRP 0x00000040UL
 #define NSCD__SHMEMHOST 0x00000080UL

+#define ASSOCIATION__SENDTO 0x00000001UL
+#define ASSOCIATION__RCVFROM 0x00000002UL
+
+#define NETLINK_KOBJECT_UEVENT_SOCKET__IOCTL 0x00000001UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__READ 0x00000002UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__WRITE 0x00000004UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__CREATE 0x00000008UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__GETATTR 0x00000010UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__SETATTR 0x00000020UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__LOCK 0x00000040UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__RELABELFROM 0x00000080UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__RELABELTO 0x00000100UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__APPEND 0x00000200UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__BIND 0x00000400UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__CONNECT 0x00000800UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__LISTEN 0x00001000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__ACCEPT 0x00002000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__GETOPT 0x00004000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__SETOPT 0x00008000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__SHUTDOWN 0x00010000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__RCVFROM 0x00020000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__SENDTO 0x00040000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__RCV_MSG 0x00080000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__SEND_MSG 0x00100000UL
+#define NETLINK_KOBJECT_UEVENT_SOCKET__NAME_BIND 0x00200000UL
+
diff -puN security/selinux/include/av_perm_to_string.h~selinux-add-support-for-netlink_kobject_ueven
--- 25/security/selinux/include/av_perm_to_string.h~selinux-add-support-for-netlink_kobject_ueven
+++ 25-akpm/security/selinux/include/av_perm_to_string.h 2005-04-12 03:21:09.245731336 -0700
@@ -118,6 +118,8 @@
 S_(SECCLASS_CAPABILITY, CAPABILITY__SYS_TTY_CONFIG, "sys_tty_config")
 S_(SECCLASS_CAPABILITY, CAPABILITY__MKNOD, "mknod")
 S_(SECCLASS_CAPABILITY, CAPABILITY__LEASE, "lease")
+ S_(SECCLASS_CAPABILITY, CAPABILITY__AUDIT_WRITE, "audit_write")
+ S_(SECCLASS_CAPABILITY, CAPABILITY__AUDIT_CONTROL, "audit_control")
 S_(SECCLASS_PASSWD, PASSWD__PASSWD, "passwd")
 S_(SECCLASS_PASSWD, PASSWD__CHFN, "chfn")
 S_(SECCLASS_PASSWD, PASSWD__CHSH, "chsh")
@@ -230,3 +232,5 @@
 S_(SECCLASS_NSCD, NSCD__SHMEMPWD, "shmempwd")
 S_(SECCLASS_NSCD, NSCD__SHMEMGRP, "shmemgrp")
 S_(SECCLASS_NSCD, NSCD__SHMEMHOST, "shmemhost")
```

Linux-Kernel: [patch 024/198] SELinux: add support for NETLINK_KOBJECT_UEVENT

```
+ S_(SECCLASS_ASSOCIATION, ASSOCIATION__SENDTO, "sendto")
+ S_(SECCLASS_ASSOCIATION, ASSOCIATION__RCVFROM, "rcvfrom")
diff -puN security/selinux/include/class_to_string.h~selinux-add-support-for-netlink_kobject_uevent
--- 25/security/selinux/include/class_to_string.h~selinux-add-support-for-netlink_kobject_uevent
+++ 25-akpm/security/selinux/include/class_to_string.h 2005-04-12 03:21:09.246731184 -0700
@@ -56,3 +56,5 @@
     S_("netlink_dnrt_socket")
     S_("dbus")
     S_("nscd")
+   S_("association")
+   S_("netlink_kobject_uevent_socket")
diff -puN security/selinux/include/flask.h~selinux-add-support-for-netlink_kobject_uevent security
--- 25/security/selinux/include/flask.h~selinux-add-support-for-netlink_kobject_uevent 2005-04-12
+++ 25-akpm/security/selinux/include/flask.h 2005-04-12 03:21:09.246731184 -0700
@@ -58,6 +58,8 @@
 #define SECCLASS_NETLINK_DNRT_SOCKET 51
 #define SECCLASS_DBUS 52
 #define SECCLASS_NSCD 53
+#define SECCLASS_ASSOCIATION 54
+#define SECCLASS_NETLINK_KOBJECT_UEVENT_SOCKET 55

/*
 * Security identifier indices for initial entities
-
-
To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to majordomo@vger.kernel.org
More majordomo info at http://vger.kernel.org/majordomo-info.html
Please read the FAQ at http://www.tux.org/lkml/
```