

Re: Apple Remote Desktop root vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-09/msg00328.html>

- *From:* Yannick von Arx <yanux@xxxxxxxx>
 - *Date:* Tue, 19 Sep 2006 23:58:56 +0200
-

It seems so that the attacker needs a ARD enabled user plus vnc password to access the client. Then he can send an install command over "Manage > Send UNIX Command"

We're talking about ARD 3.0 so we've got the new feature to lock client's screen with a message. From my point of view it's not a vulnerability in ARD, just an insecure point.

Regards,
Yannick von Arx

On 19.09.2006, at 19:32, Erik Lat wrote:

So in order for this vulnerability to be exploited, the attacker needs to have a local account on the machine correct? Your exploitation explanation is a bit construed. Any more info / demonstrations would be helpful.

–Erik

On 18 Sep 2006 21:26:52 –0000
fribitch@xxxxxxxxxxxx wrote:

Background:

ARD allows unix commands to be remotely sent from an admin workstation. These commands can be run as root, because the ard administrator can be given sudo access. This exploit involves sending a unix command as root to install a package that was copied to /tmp/. In this case, the app is Adobe CS 2.0 using the adobe silent installation script. The script will mount disk images as root, run the install, then cleanup. If a standard user is logged in, they will see an icon on the dock for the install, but should never see anything besides the icon.

The issue:

The process LoginWindow is owned by the logged in user. If the system is at the login window, then the process LoginWindow is owned by root. If the system is mounting a disk image visible only to root, then the image will try to appear on the desktop. Clicking the mouse will force the desktop to appear, as well as the menus. A user sitting that the system will then see a

Re: Apple Remote Desktop root vulnerability

finder window, and the root users home directory. The login window can be ignored, and the user has full root access. Files can be deleted without authentication, and the trash can be emptied. If a user tries to login, the login window will check their credentials, but they will end up logging in to the root desktop with root privileges.

The workaround:

If you are trying to run a remote install script such as the Adobe Silent installer, use the lock screen feature in ARD. This locks the users desktop until the admin is done doing their thing.

The end result:

<http://www.flickr.com/photos/metfoo/246858852/>

Adobes script:

```
#!/bin/sh
#
# Example script to run the Adobe Creative Suite 2 Installer silently.
#
#
# Copyright: 2005 Adobe Systems, Inc.
#
#

function detach_images
{
# unmount any previous mounted installer images
for NUMBER in 1 2 3 4
do
MOUNTED_POINT="/Volumes/Adobe Creative Suite Disk ${NUMBER} "
/sbin/mount |/usr/bin/grep "${MOUNTED_POINT}" 2>/dev/null
if [ $? -eq 0 ]; then
echo "Another \"${MOUNT_POINT}\" already attached."
DEVICE=`/sbin/mount |/usr/bin/grep "${MOUNTED_POINT}" 2>/dev/ null
|/usr/bin/cut -d" " -f1`
if [ -b "${DEVICE}" ]; then
/usr/bin/hdiutil detach "${DEVICE}"
echo "Detaching \"${DEVICE}\"..."
fi
fi
done
}

SAVEDIR="`pwd`"
trap 'cd "${SAVEDIR}"' EXIT

if [ $# -ne 2 ]; then
echo "usage: $0 <image folder> <config filepath>"
```

Re: Apple Remote Desktop root vulnerability

```
exit 1
fi

IMGDIR=$1
CONFIG=$2

# Check OS Version, Minimum is 10.2.8
OSVERSION=`/usr/bin/sw_vers |/usr/bin/grep ProductVersion |/usr/bin/cut
-d: -f2`
MAJORVER=`echo ${OSVERSION} |/usr/bin/cut -d . -f2`
MVTEMP=`echo ${OSVERSION} |/usr/bin/cut -d. -f3`
MINORVER=${MVTEMP:-0}

if [ ${MAJORVER} -lt 3 ] ; then
# if less than 10.3
if [ ${MAJORVER} -ne 2 ] ; then
echo "This version of MacOS (${OSVERSION}) is not supported."
exit 1;
else
if [ ${MINORVER} -lt 8 ] ; then
echo "This version of MacOS (${OSVERSION}) is not supported."
exit 1;
fi
fi
HDIUTIL_OPTIONS=
else
# additional hdiutil options for 10.3 or above system
HDIUTIL_OPTIONS="-private -noverify"
fi

# Check root volume is HFS
/sbin/mount -t hfs |/usr/bin/grep " / " 2>/dev/null
if [ $? -ne 0 ] ; then
echo "Root volume is not a HFS volume."
exit 5
fi

# validate the arguments
if [ ! -d "$IMGDIR" ] ; then
echo "$IMGDIR" does not exist.
exit 2
fi

if [ ! -r "$CONFIG" ] ; then
echo "$CONFIG" does not exist.
exit 3
fi
```

Re: Apple Remote Desktop root vulnerability

```
# Check running as root
MYUID=`/usr/bin/id -u`

if [ ${MYUID} -ne 0 ] ; then
echo "You need to be root to run the Adobe Creative Suite 2 Installer."
exit 4
fi

cd "${IMGDIR}"
IMGCOUNT=`/bin/ls -l *.dmg 2>/dev/null | /usr/bin/wc -l`
if [ -z "${IMGCOUNT}" -o "${IMGCOUNT}" = "0" ] ; then
echo "No disk image found in "${IMGDIR}"."
exit 2
fi

#detach any already attached installer images
detach_images

# Mount the disk images for the installer CDs
for DMG in *.dmg
do
# mount the remaining disk images
echo
echo "---- Attaching Installer disk image ${NUMBER}..."
echo /usr/bin/hdiutil attach -verbose -readonly $ {HDIUTIL_OPTIONS}
"${DMG}"
/usr/bin/hdiutil attach -verbose -readonly ${HDIUTIL_OPTIONS} "${DMG}"

if [ $? -ne 0 ] ; then
echo "Error in attaching installer disk image: \"${DMG}\""
exit 6
fi
done

echo
echo
echo "----- Starting the Adobe Creative Suite Installer..."
echo
"/Volumes/Adobe Creative Suite Disk 1/Adobe Installer.app/Contents/
MacOS/Adobe Installer" --batch -c "${CONFIG}"
INSTALLATION_RESULT=$?
echo

#now detach attached installer images
detach_images

exit ${INSTALLATION_RESULT}
```

Re: Apple Remote Desktop root vulnerability

--

Erik Lat
System Engineer
Lextech Global Services

--

e-mail: yannick.vonarx@xxxxxxxxx
web: <http://www.yanux.ch>