Prueba de Escalada de Privilegios

Detalles Técnicos

Sistema Operativo: EducaAndOs (Versión Normal) Distribución Basada: Ubuntu Linux 20.04 (TLS) MD5 ISO: cf64af133f88435cd878a048b9fd1885 Espacio de Disco asignado: 40960 MBytes RAM asignada: 4096 MBytes Host de virtualización: VirtualBox for Linux 6.1 Tipo de SO: x64 bits Sistema de Ventanas: x11 Versión de GNOME: 3.36.3

Objetivos y descripción

Se va a realizar la prueba de escalada de privilegios sobre el sistema operativo EducaAndOs, los fallos encontrados pueden que no sean revelantes o que en la realidad no sean de importancia, pero deben ser resueltos para conseguir un sistema seguro. La finalidad de esta prueba es asegurar que el sistema operativo, no tiene ningun agujero de seguridad y que no es una entrada para posibles ataques a redes con este sistema implantado y/o asegurar la integridad de los archivos confidenciales que se puedan almacenar en equipos con este sistema implantado.

Información adicional

El sistema estará conectado a internet durante toda la prueba y se relizarán las actualizaciones pendientes. Para poder asegurar la integridad de este sistema y del equipo en el que se realize esta prueba, esta prueba se ha realizado en un entorno seguro y virtual.

PoC

Información sobre el software y sistema

Centro de Software de EducaAndOs: 3.36.1 Distributor ID: Educaandos Description: EducaAndOS 20.04 Release: 20.04 Codename: focal Kernel Name: Linux Nodename: educaandos Kernel Version: 5.4.0-66-generic Machine: x86_64 Operating System: GNU/Linux

```
$ cat /proc/version

Linux version 5.4.0-66-generic (buildd@lgw01-amd64-039) (gcc version 9.3.0 (Ubuntu
9.3.0-17ubuntu1~20.04)) #74-Ubuntu SMP Wed Jan 27 22:54:38 UTC 2021

$ echo $PATH

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
14-oracle/bin:/usr/lib/jvm/java-14-oracle/db/bin

$ (env || set) 2>/dev/null

SHELL=/bin/bash
SESSION_MANAGER=local/educaandos:@/tmp/.ICE-unix/1549,unix/educaandos:/tmp/.ICE-
unix/1549
QT_ACCESSIBILITY=1
```

```
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GTK_IM_MODULE=ibus
DERBY_HOME=/usr/lib/jvm/java-14-oracle/db
GTK2_MODULES=overlay-scrollbar
LANGUAGE=es_ES:
QT4_IM_MODULE=ibus
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
JAVA_HOME=/usr/lib/jvm/java-14-oracle
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1416
GTK_MODULES=gail:atk-bridge
PWD=/home/usuario
LOGNAME=usuario
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
J2REDIR=/usr/lib/jvm/java-14-oracle
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/usuario
USERNAME=usuario
IM_CONFIG_PHASE=1
LANG=es_ES.UTF-8
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/fdb2612a_900c_4ab6_9735_a4c0bd3d052b
INVOCATION_ID=c2ca7b253f2b4a7aacc46daa57a6596c
MANAGERPID=1236
CLUTTER_IM_MODULE=ibus
GJS_DEBUG_OUTPUT=stderr
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
J2SDKDIR=/usr/lib/jvm/java-14-oracle
LESSOPEN=| /usr/bin/lesspipe %s
USER=usuario
GNOME_TERMINAL_SERVICE=:1.128
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:27975
XDG_DATA_DIRS=/usr/share/eos:/usr/share/ubuntu:/usr/local/share/:/usr/share/
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
```

```
14-oracle/bin:/usr/lib/jvm/java-14-oracle/db/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus_=/usr/bin/env

$ cat /etc/os-release 2>/dev/null

NAME="EducaAndOS"
VERSION="20.04"
ID=educaandos
ID_LIKE=debian
PRETTY_NAME="EducaAndOS 20.04"
VERSION_ID="20.04"
HOME_URL="https://www.guadalinexedu.org/"
SUPPORT_URL="https://www.guadalinexedu.org/"
BUG_REPORT_URL="https://bugs.launchpad.net/guadalinexedu/"
PRIVACY_POLICY_URL="https://www.guadalinexedu.org/"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

!ATENCION¡¡: Se ha realizado un escaneo con un potente script de analisis, la respuesta es demasiado larga, por ello hay un archivo .txt que representa la salida de la consola de este script en el que descubren diferentes vulnerabilidades en las herramientas instaladas por defecto en la distribución. Revisar el archivo output.txt para mas información

Conclusion

El sistema tiene multiples puntos vulnerables, la mayoria de ellos contemplan vulnerabilidades criticas. Para cualquier contacto:

https://linktr.ee/nuofrwk Email: pabloarrabal@nuoframework.ml Email2: nuoframework@protonmail.com