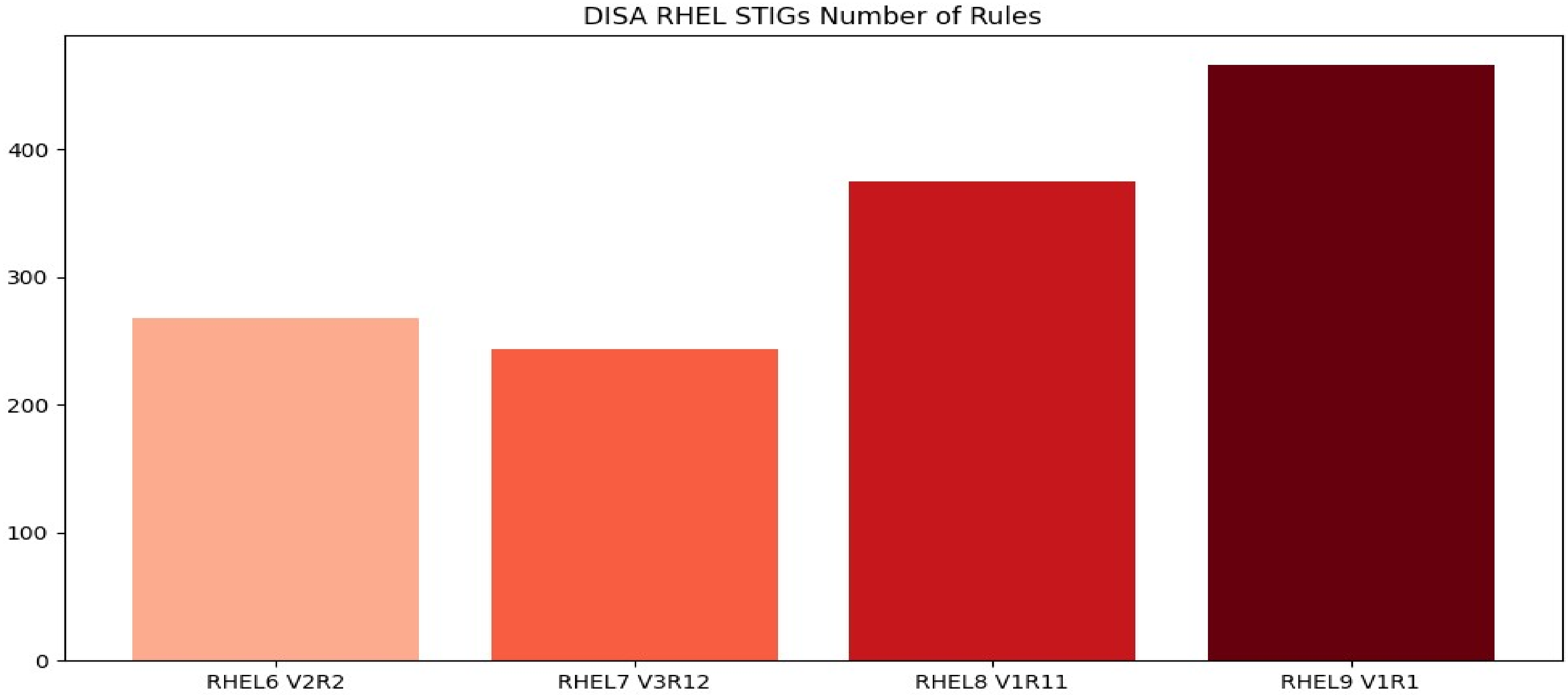
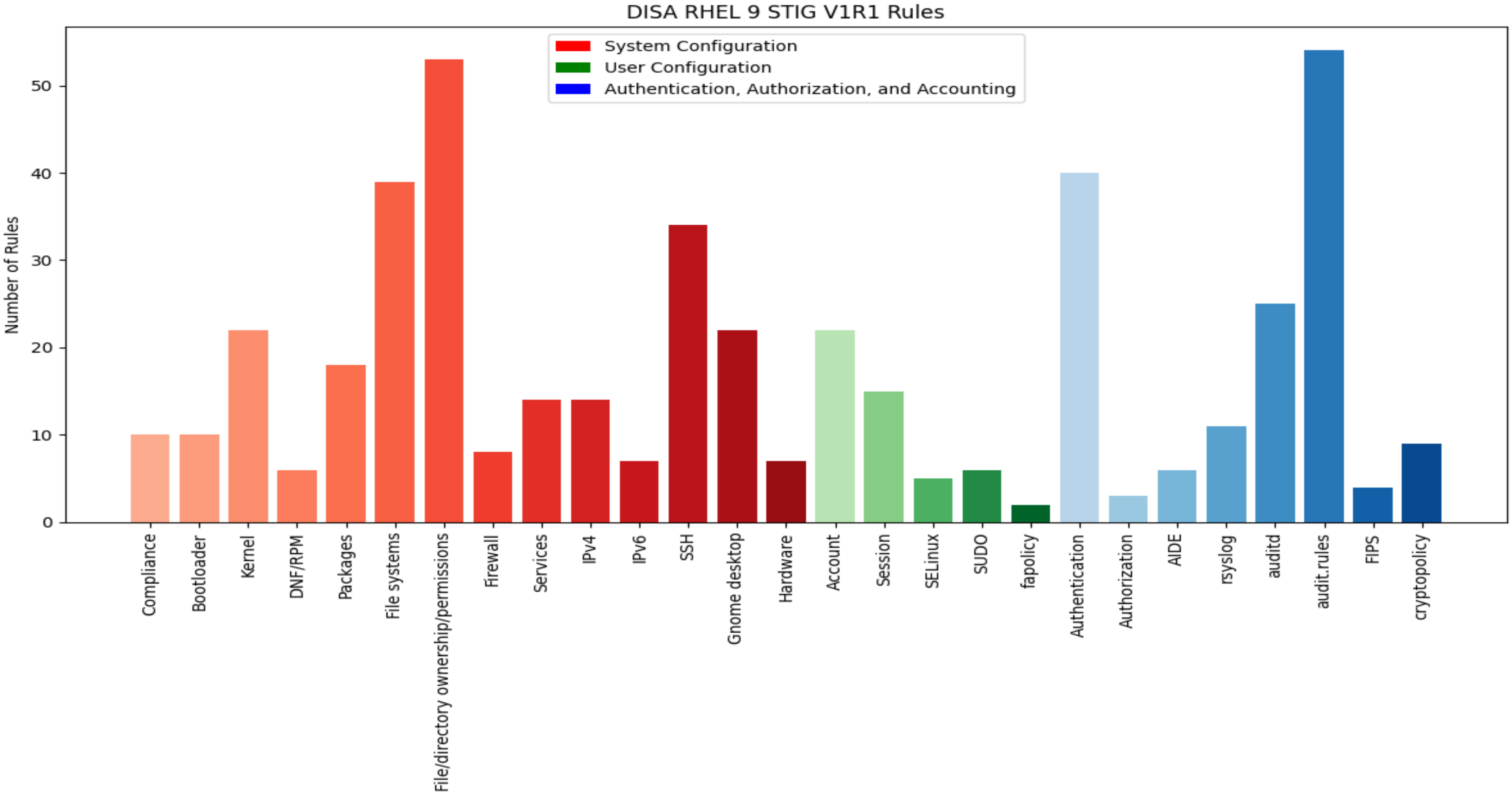
Bitching about the RHEL STIG
And other ramblings

@JayFoxtrot

RHEL STIG Requirement creep



RHEL 9 Rules by Category



STIG Severity

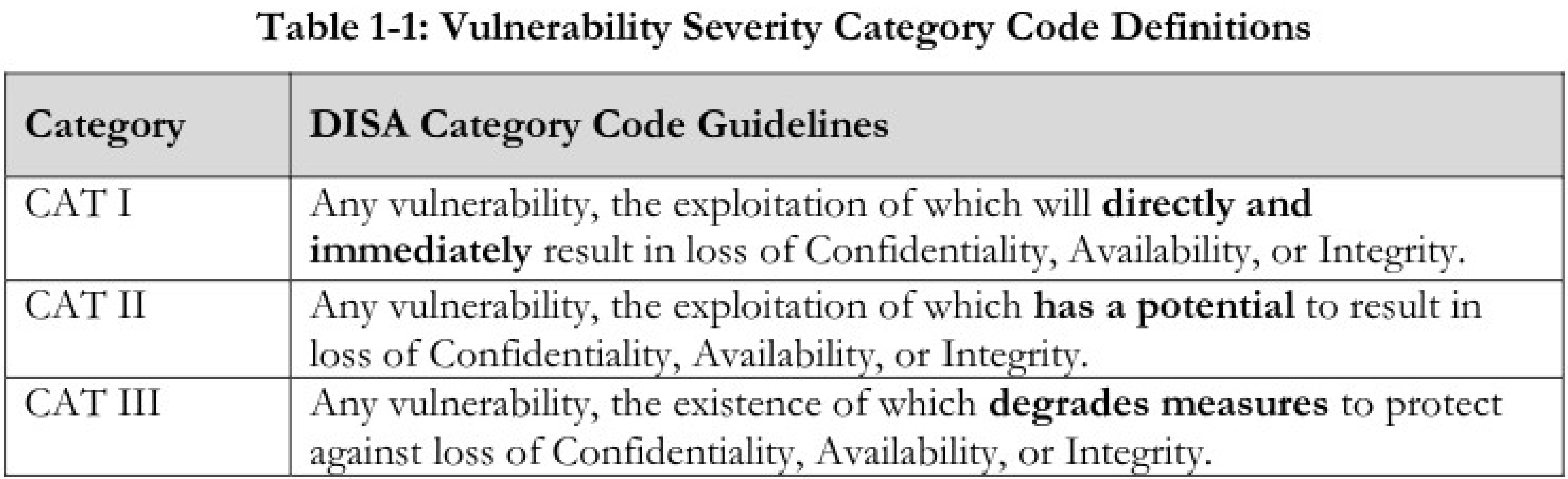
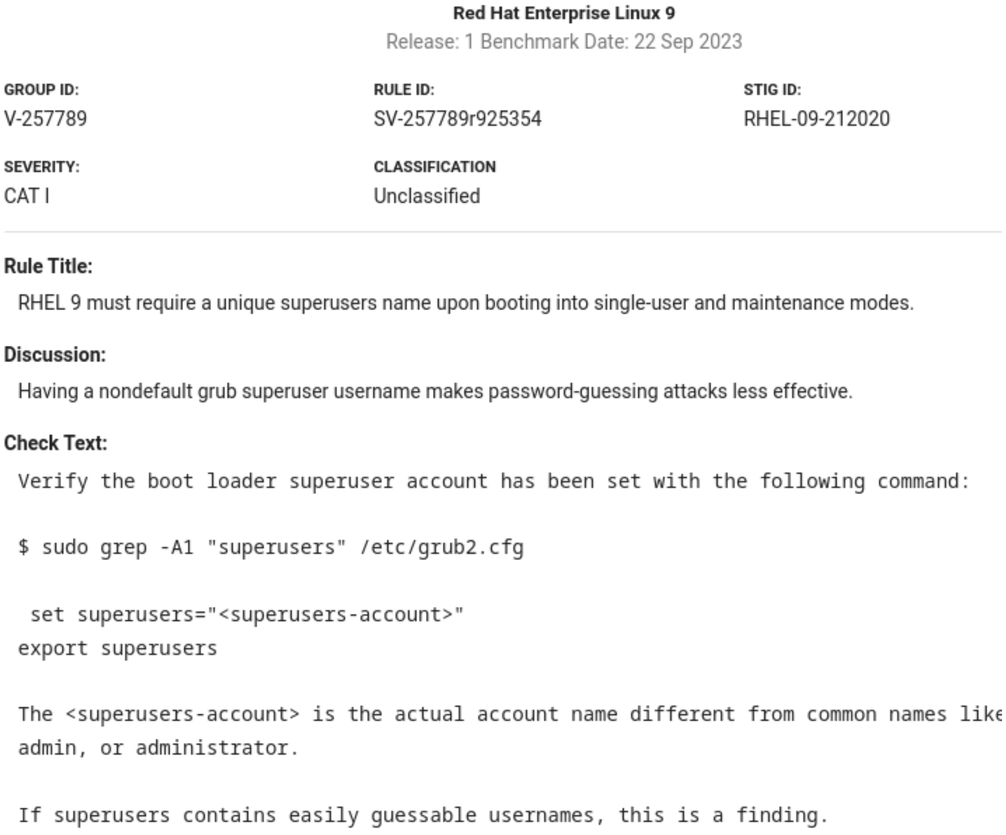


Table 1-1: Vulnerability Severity Category Code Definitions

Category	**DISA Category Code Guidelines**
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

RHEL 9 STIG



Red Hat Enterprise Linux 9
Release: 1 Benchmark Date: 22 Sep 2023

GROUP ID:	RULE ID:	STIG ID:
V-257789	SV-257789r925354	RHEL-09-212020
SEVERITY:	**CLASSIFICATION**	
CAT I	Unclassified	

Rule Title:

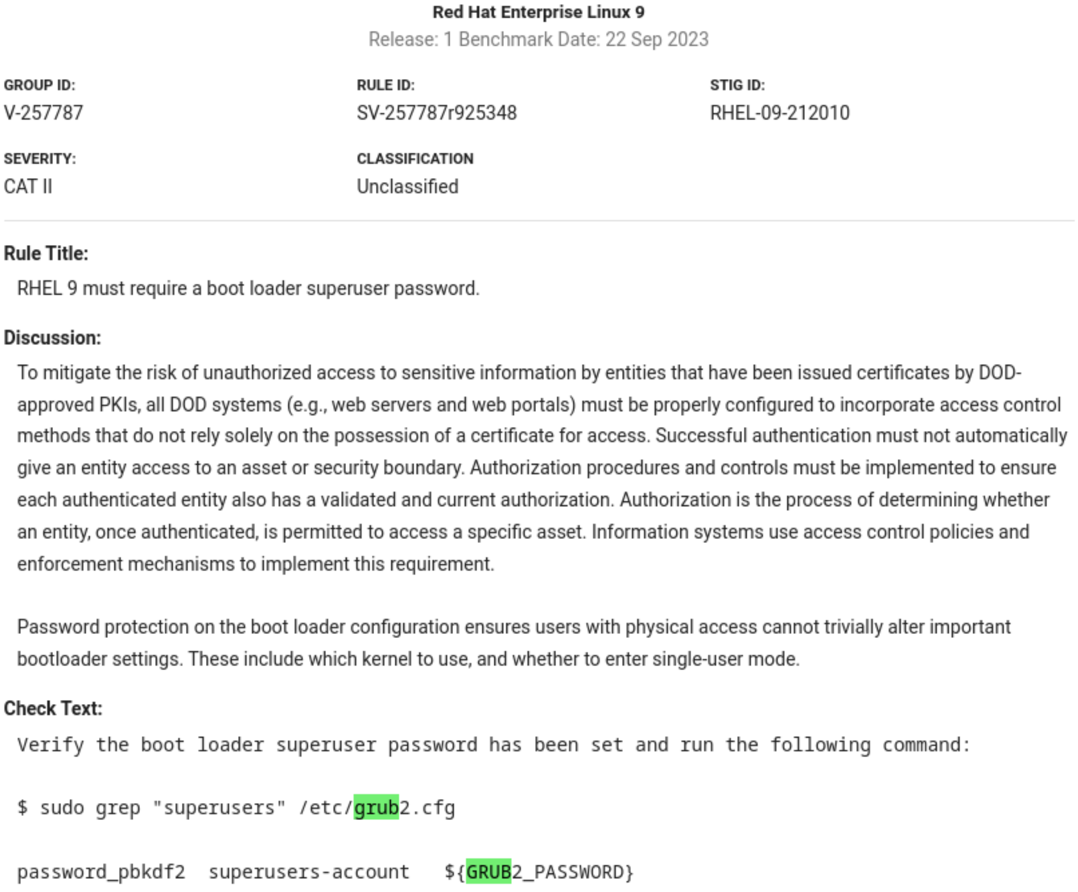
RHEL 9 must require a unique superusers name upon booting into single-user and maintenance modes.

Discussion:

Having a nondefault grub superuser username makes password-guessing attacks less effective.

Check Text:

```
Verify the boot loader superuser account has been set with the following command:

$ sudo grep -A1 "superusers" /etc/grub2.cfg

 set superusers="<superusers-account>"
export superusers

The <superusers-account> is the actual account name different from common names like
admin, or administrator.

If superusers contains easily guessable usernames, this is a finding.
```



Red Hat Enterprise Linux 9
Release: 1 Benchmark Date: 22 Sep 2023

GROUP ID:	RULE ID:	STIG ID:
V-257787	SV-257787r925348	RHEL-09-212010
SEVERITY:	**CLASSIFICATION**	
CAT II	Unclassified	

Rule Title:

RHEL 9 must require a boot loader superuser password.

Discussion:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Password protection on the boot loader configuration ensures users with physical access cannot trivially alter important bootloader settings. These include which kernel to use, and whether to enter single-user mode.

Check Text:

```
Verify the boot loader superuser password has been set and run the following command:

$ sudo grep "superusers" /etc/grub2.cfg

password_pbkdf2  superusers-account   ${GRUB2_PASSWORD}
```

grub2 username /password

- Password stored in a separate file in RHEL/Fedora
- Called user.cfg
- In RHEL8 just delete or rename user.cfg file from EFI partition
- On RHEL9/Fedora a little more complicated

grub2 user.cfg example

```
Example:
root@system1:~# find /boot -name user.cfg | xargs cat
GRUB2_PASSWORD=grub.pbkdf2.sha512.10000.FF26431B77CFC9BADBD
EF7F8DEF5684997EDCE2C7797D35A760B1D8CF276737E0C312D92C2AE21
9B0921D1719A9A47317D37C4C6EE4F4D45E235911259421A7D.A40AAD92
E26A1DBC1FE7FC95000073D49150BBAC20F2EDB5C3F08F098476939378A
AB9023DD657CD12E7680E94B906B43C7D24F1668A0E6453453C50556383
AE
```

What are we bypassing?

```
root@system1:~# find /boot -name grub.cfg -ls
4 -rwx------   1 root     root          146 Dec 31 22:22
/boot/efi/EFI/fedora/grub.cfg
8 -rwx------   1 root     root         6825 Dec 31 21:02
/boot/grub2/grub.cfg
```

```
root@system1:~# cat /boot/efi/EFI/fedora/grub.cfg
search --no-floppy --fs-uuid --set=dev 40a48cb0-a44b-49de-a7c0-
db5adb726b5f
set prefix=($dev)/grub2
export $prefix
configfile $prefix/grub.cfg
```

What are we bypassing?

```
Prefix is used in several places
When “configfile” loads the real grub:
```

```
root@system1:/home/jeremy# grep prefix /boot/grub2/grub.cfg
elif [ -s $prefix/grubenv ]; then
if [ -f ${prefix}/user.cfg ]; then
  source ${prefix}/user.cfg
elif [ -z "${config_directory}" -a -f  $prefix/custom.cfg ]; then
  source $prefix/custom.cfg
```

What are we bypassing?

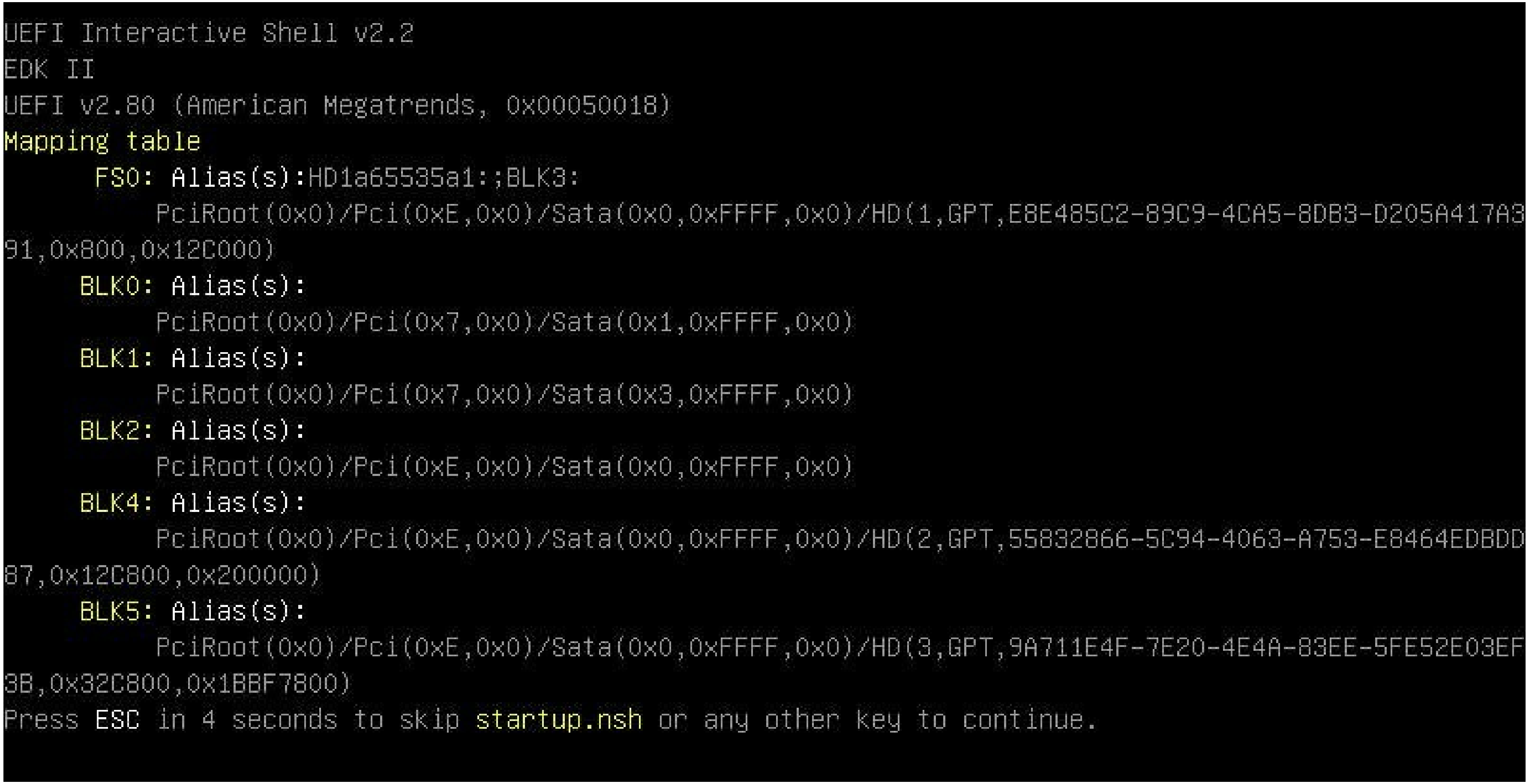
Mainly in this section:

```
### BEGIN /etc/grub.d/01_users ###
if [ -f ${prefix}/user.cfg ]; then
  source ${prefix}/user.cfg
  if [ -n "${GRUB2_PASSWORD}" ]; then
    set superusers="root"
    export superusers
    password_pbkdf2 root ${GRUB2_PASSWORD}
  fi
fi
### END /etc/grub.d/01_users ###
```

UEFI Shell

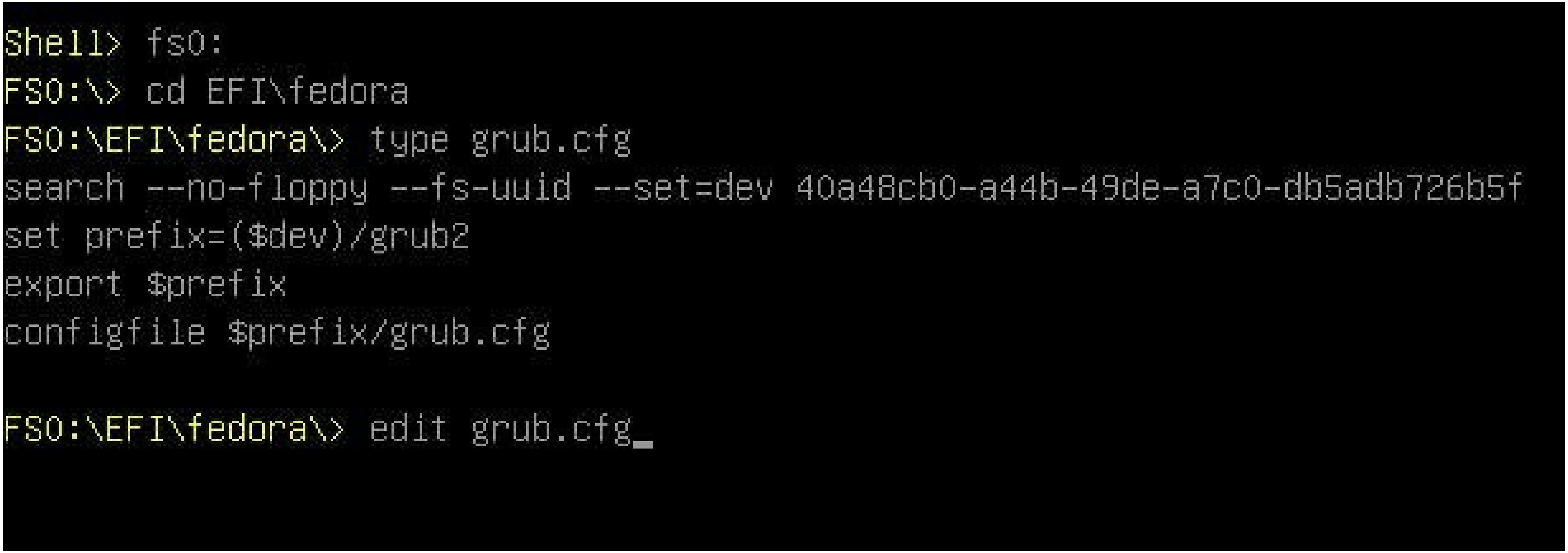
- Lots of functionality to manipulate files on a FAT32 partition
- EFI uses a FAT32 partition
- Manipulate grub files
- Seems to be gone form Dell servers
- Only works when not in secure boot on Supermicro servers

UEFI Shell - Boot



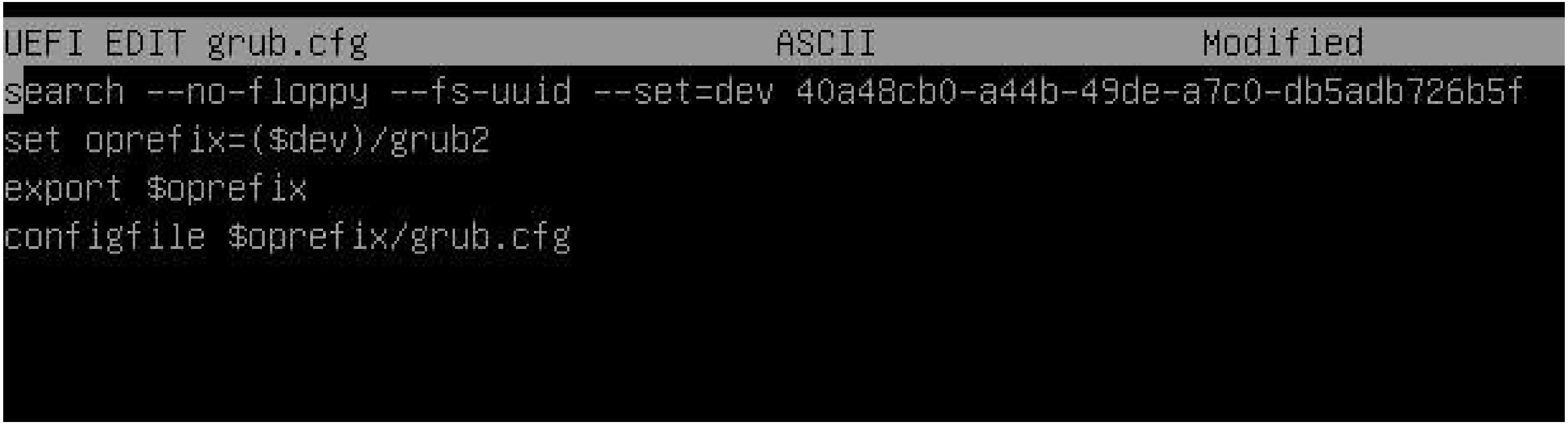
```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.80 (American Megatrends, 0x00050018)
Mapping table
      FS0: Alias(s):HD1a65535a1:;BLK3:
          PciRoot(0x0)/Pci(0xE,0x0)/Sata(0x0,0xFFFF,0x0)/HD(1,GPT,E8E485C2-89C9-4CA5-8DB3-D205A417A3
91,0x800,0x12C000)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x7,0x0)/Sata(0x1,0xFFFF,0x0)
     BLK1: Alias(s):
          PciRoot(0x0)/Pci(0x7,0x0)/Sata(0x3,0xFFFF,0x0)
     BLK2: Alias(s):
          PciRoot(0x0)/Pci(0xE,0x0)/Sata(0x0,0xFFFF,0x0)
     BLK4: Alias(s):
          PciRoot(0x0)/Pci(0xE,0x0)/Sata(0x0,0xFFFF,0x0)/HD(2,GPT,55832866-5C94-4063-A753-E8464EDBDD
87,0x12C800,0x200000)
     BLK5: Alias(s):
          PciRoot(0x0)/Pci(0xE,0x0)/Sata(0x0,0xFFFF,0x0)/HD(3,GPT,9A711E4F-7E20-4E4A-83EE-5FE52E03EF
3B,0x32C800,0x1BBF7800)
Press ESC in 4 seconds to skip startup.nsh or any other key to continue.
```

UEFI Shell - edit grub.cfg



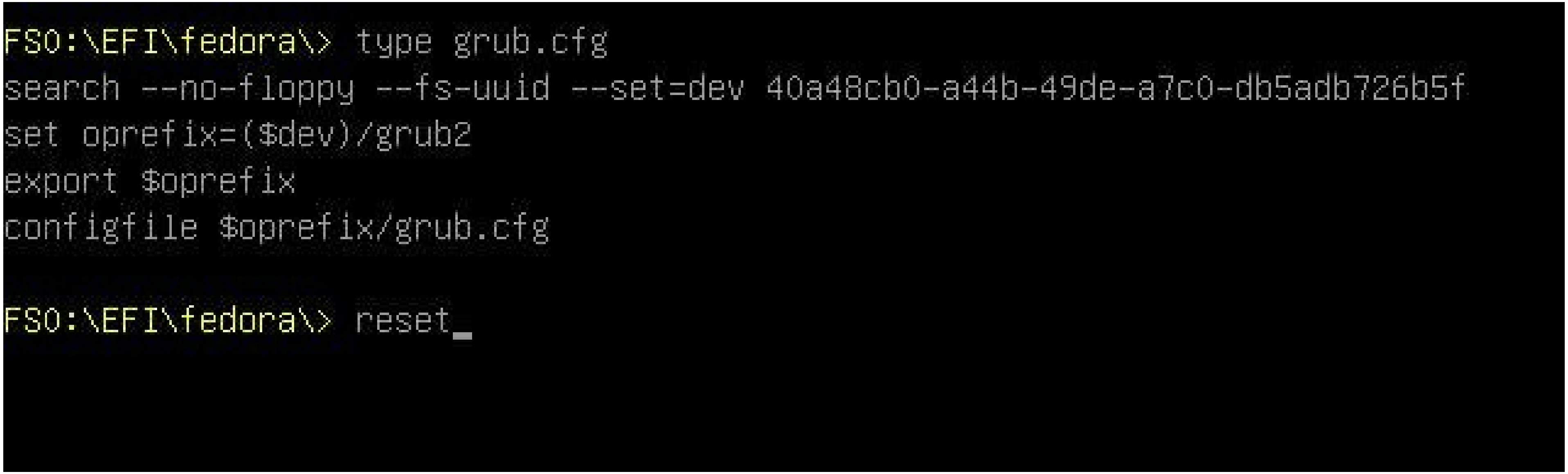
```
Shell> fs0:
FS0:\> cd EFI\fedora
FS0:\EFI\fedora\> type grub.cfg
search --no-floppy --fs-uuid --set=dev 40a48cb0-a44b-49de-a7c0-db5adb726b5f
set prefix=($dev)/grub2
export $prefix
configfile $prefix/grub.cfg

FS0:\EFI\fedora\> edit grub.cfg_
```

UEFI Shell – change prefix



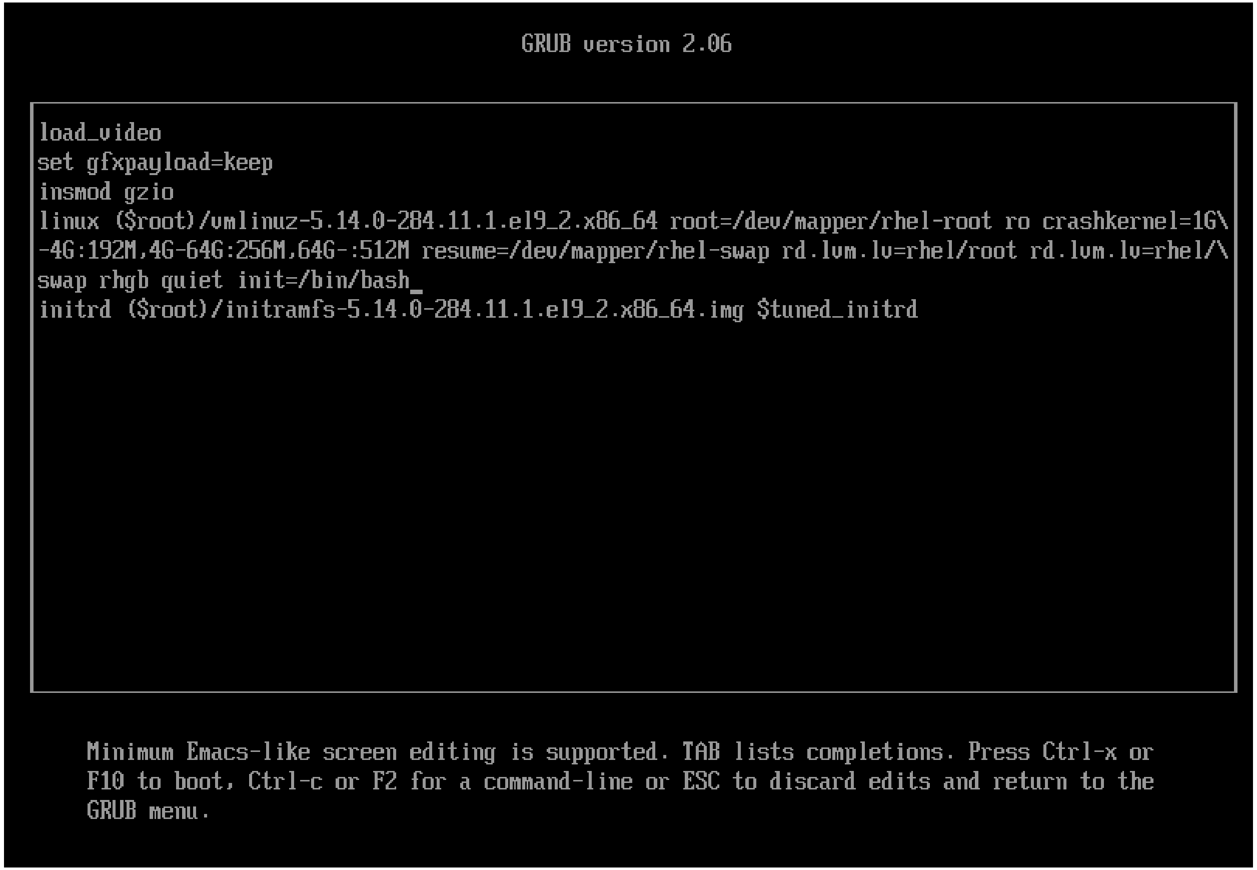
```
UEFI EDIT grub.cfg                                     ASCII                              Modified
search --no-floppy --fs-uuid --set=dev 40a48cb0-a44b-49de-a7c0-db5adb726b5f
set oprefix=($dev)/grub2
export $oprefix
configfile $oprefix/grub.cfg
```

UEFI Shell - reboot



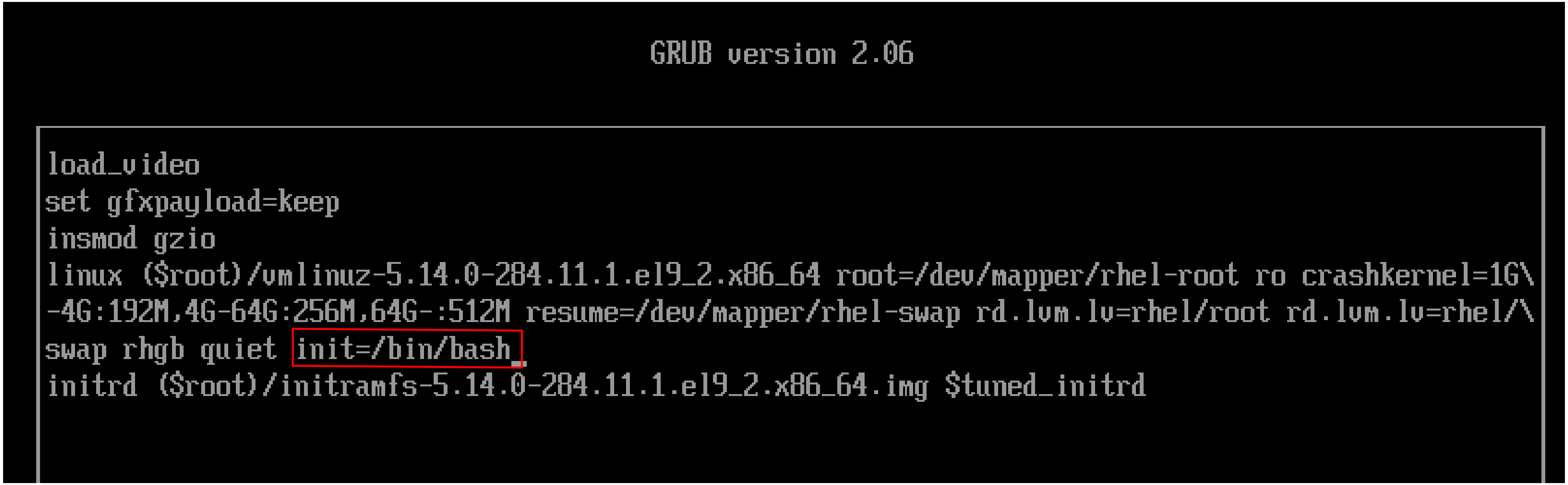
```
FS0:\EFI\fedora\> type grub.cfg
search --no-floppy --fs-uuid --set=dev 40a48cb0-a44b-49de-a7c0-db5adb726b5f
set oprefix=($dev)/grub2
export $oprefix
configfile $oprefix/grub.cfg

FS0:\EFI\fedora\> reset_
```

Use bash for init



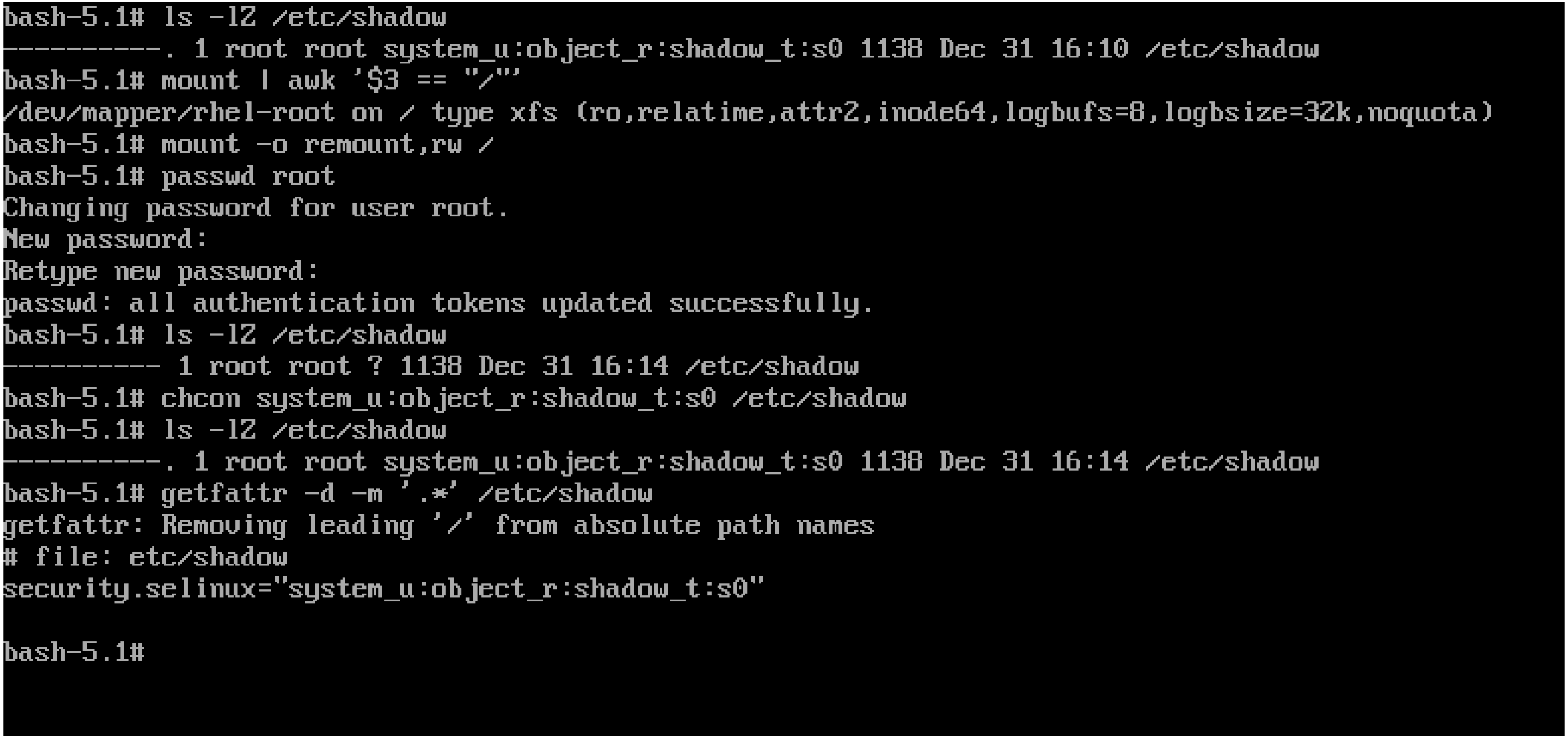
```
GRUB version 2.06

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-284.11.1.el9_2.x86_64 root=/dev/mapper/rhel-root ro crashkernel=1G\
-4G:192M,4G-64G:256M,64G-:512M resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/\
swap rhgb quiet init=/bin/bash_
initrd ($root)/initramfs-5.14.0-284.11.1.el9_2.x86_64.img $tuned_initrd

    Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or
    F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the
    GRUB menu.
```

Use bash for init



```
GRUB version 2.06

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-284.11.1.el9_2.x86_64 root=/dev/mapper/rhel-root ro crashkernel=1G\
-4G:192M,4G-64G:256M,64G-:512M resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/\
swap rhgb quiet init=/bin/bash_
initrd ($root)/initramfs-5.14.0-284.11.1.el9_2.x86_64.img $tuned_initrd
```

Change the root password



```
bash-5.1# ls -lZ /etc/shadow
----------. 1 root root system_u:object_r:shadow_t:s0 1138 Dec 31 16:10 /etc/shadow
bash-5.1# mount | awk '$3 == "/"'
/dev/mapper/rhel-root on / type xfs (ro,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota)
bash-5.1# mount -o remount,rw /
bash-5.1# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
bash-5.1# ls -lZ /etc/shadow
---------- 1 root root ? 1138 Dec 31 16:14 /etc/shadow
bash-5.1# chcon system_u:object_r:shadow_t:s0 /etc/shadow
bash-5.1# ls -lZ /etc/shadow
----------. 1 root root system_u:object_r:shadow_t:s0 1138 Dec 31 16:14 /etc/shadow
bash-5.1# getfattr -d -m '.*' /etc/shadow
getfattr: Removing leading '/' from absolute path names
# file: etc/shadow
security.selinux="system_u:object_r:shadow_t:s0"

bash-5.1#
```

Consequences

- No logs
  - /bin/bash isn’t systemd won’t start logging
    - System is booted read only initially anyways
  - Confidentiality, Integrity, and Availability all compromised

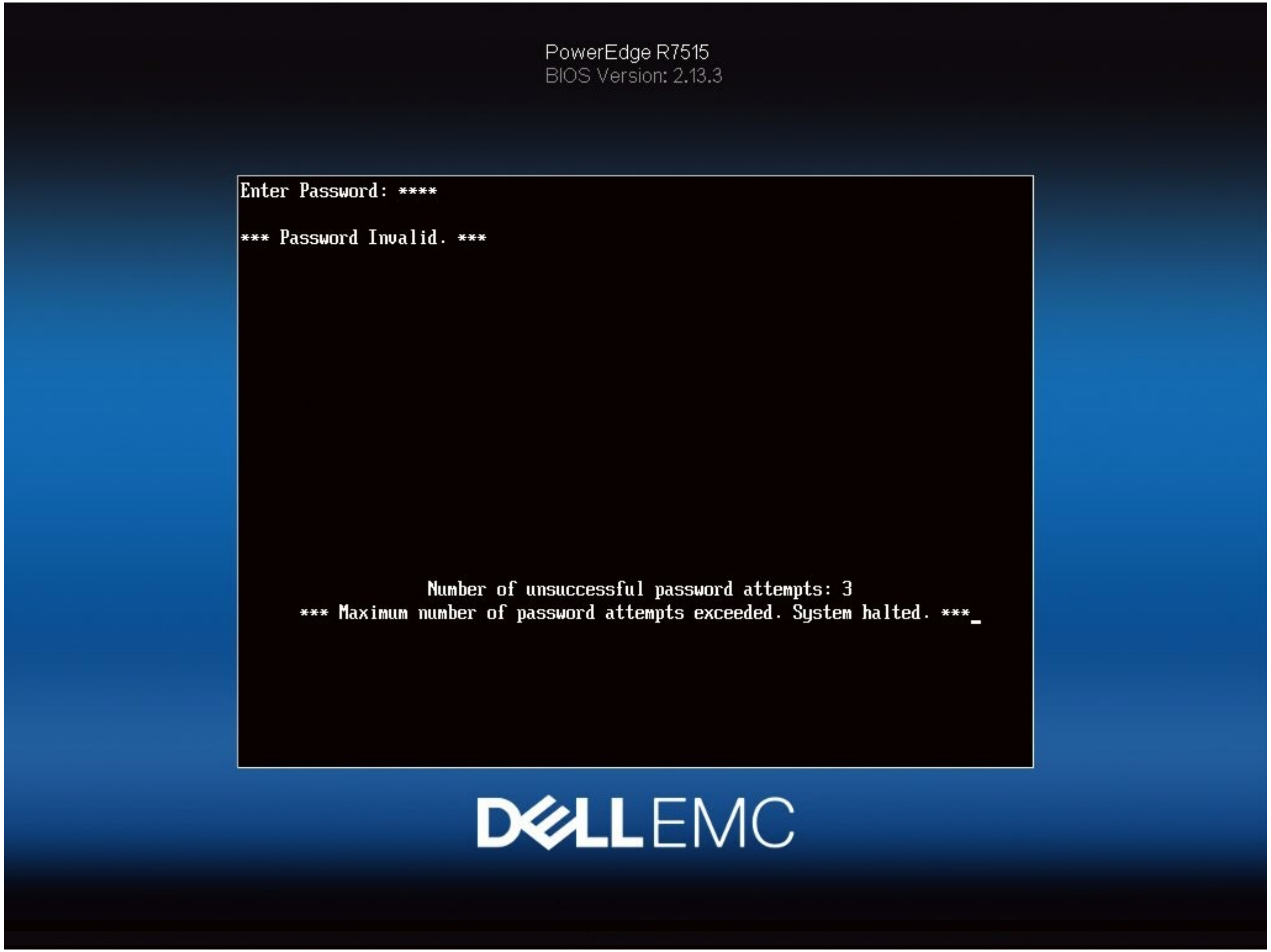
Prevention

- Password protected BIOS/UEFI
- Secure boot
- Measured boot
- Disk Encryption
  - TPM unlock
    - Not flawless: https://pulsesecurity.co.nz/advisories/tpm-luks-bypass

Dell Server Locked out

- Dealing with a locked out setup/system password
- Use iDRAC to remove the setting from the BIOS

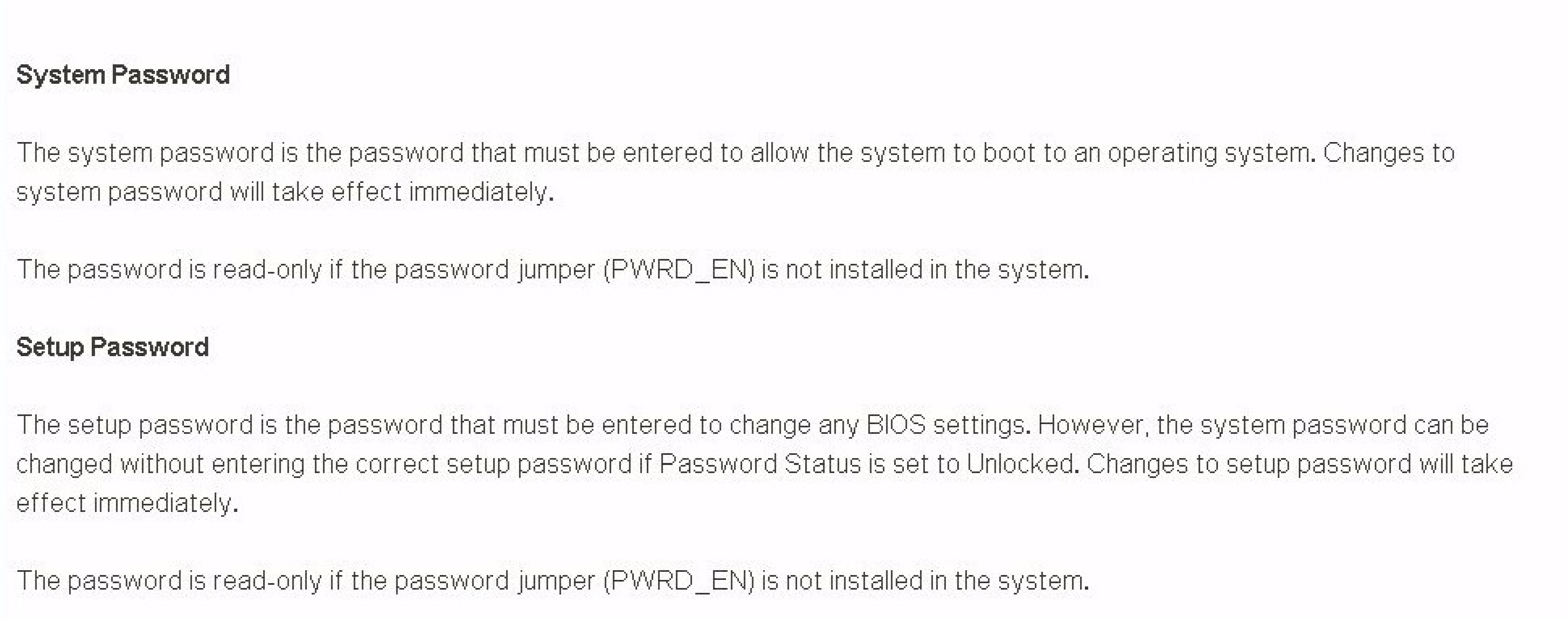
Dell Setup and System Password



PowerEdge R7515
BIOS Version: 2.13.3

```
Enter Password: ****

*** Password Invalid. ***

                    Number of unsuccessful password attempts: 3
      *** Maximum number of password attempts exceeded. System halted. ***_
```

Dell Setup and System Password



System Password

The system password is the password that must be entered to allow the system to boot to an operating system. Changes to system password will take effect immediately.

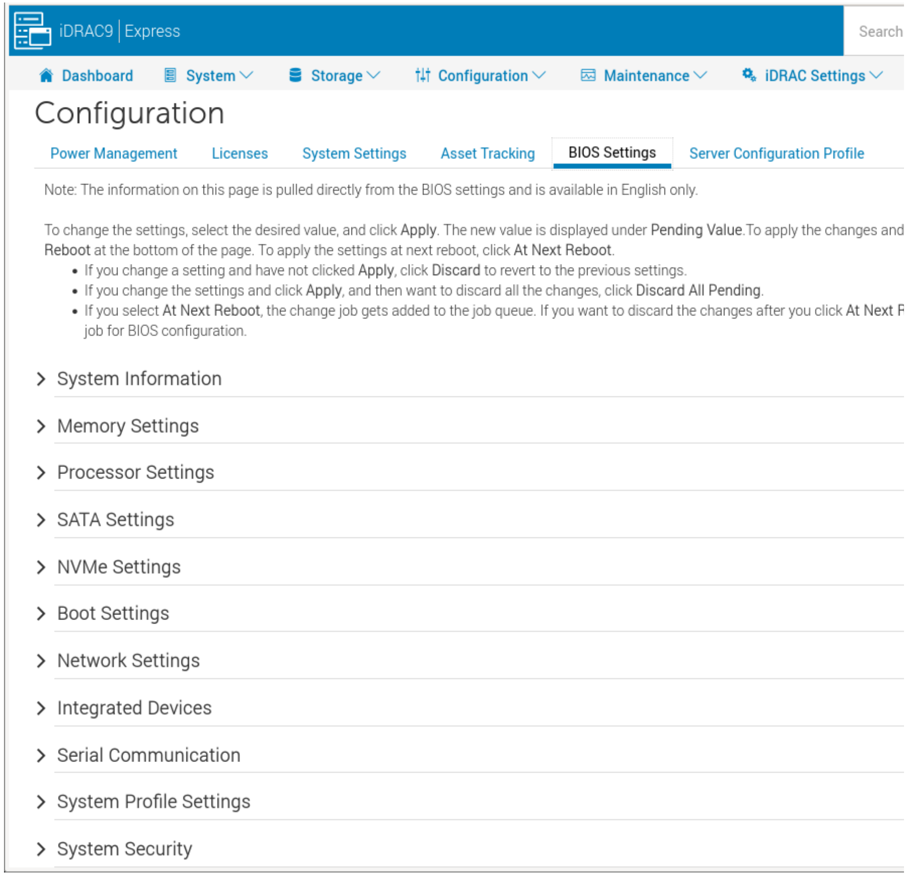
The password is read-only if the password jumper (PWRD_EN) is not installed in the system.

Setup Password

The setup password is the password that must be entered to change any BIOS settings. However, the system password can be changed without entering the correct setup password if Password Status is set to Unlocked. Changes to setup password will take effect immediately.

The password is read-only if the password jumper (PWRD_EN) is not installed in the system.

Dell Setup and System Password

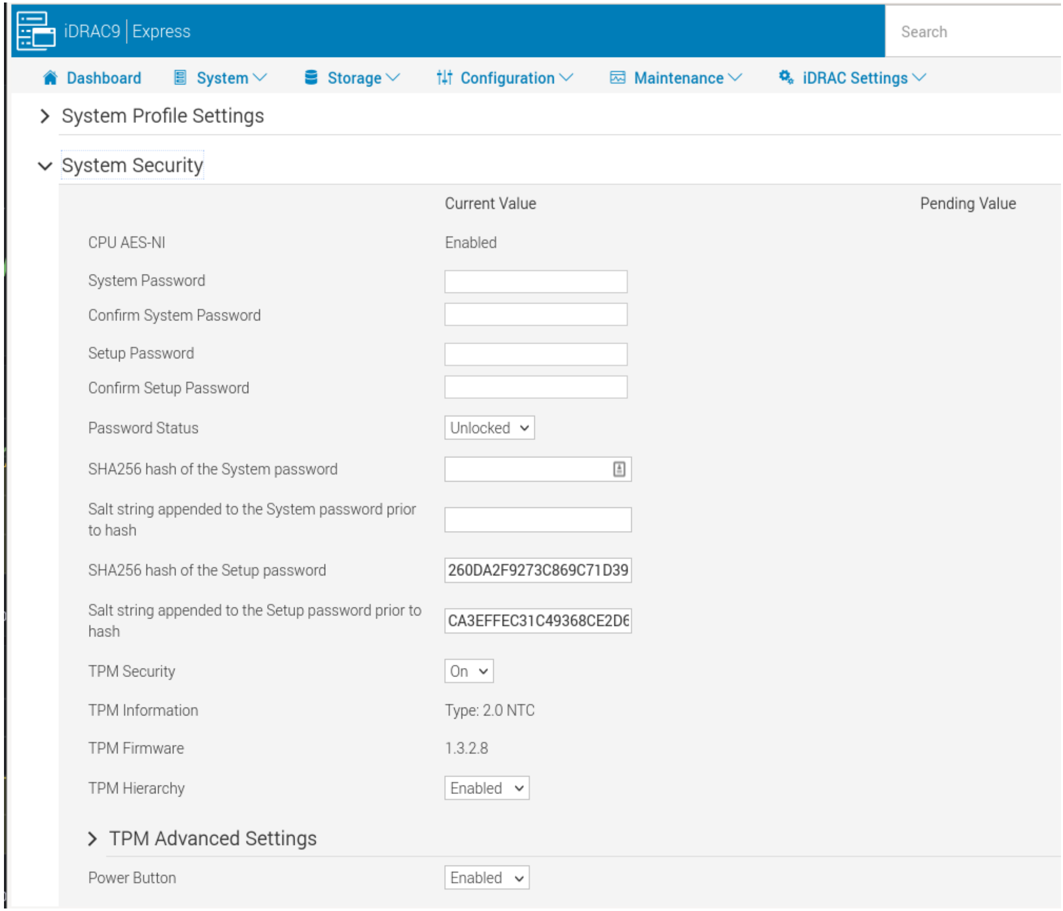


Configuration

Note: The information on this page is pulled directly from the BIOS settings and is available in English only.

To change the settings, select the desired value, and click **Apply**. The new value is displayed under **Pending Value**.To apply the changes and **Reboot** at the bottom of the page. To apply the settings at next reboot, click **At Next Reboot**.

- If you change a setting and have not clicked **Apply**, click **Discard** to revert to the previous settings.
- If you change the settings and click **Apply**, and then want to discard all the changes, click **Discard All Pending**.
- If you select **At Next Reboot**, the change job gets added to the job queue. If you want to discard the changes after you click **At Next F** job for BIOS configuration.



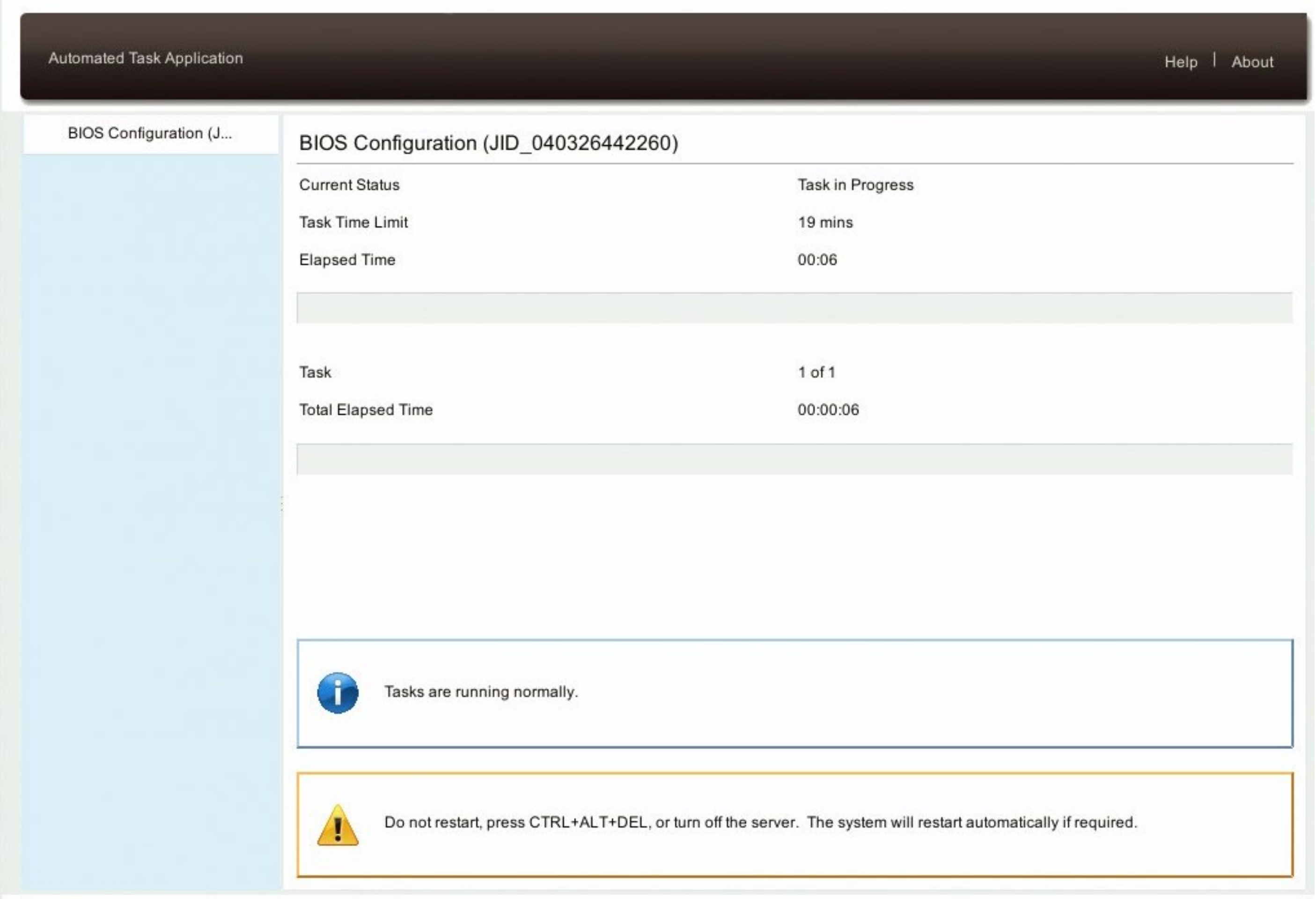
	Current Value	Pending Value
CPU AES-NI	Enabled	
System Password		
Confirm System Password		
Setup Password		
Confirm Setup Password		
Password Status	Unlocked	
SHA256 hash of the System password		
Salt string appended to the System password prior to hash		
SHA256 hash of the Setup password	260DA2F9273C869C71D39	
Salt string appended to the Setup password prior to hash	CA3EFFEC31C49368CE2D6	
TPM Security	On	
TPM Information	Type: 2.0 NTC	
TPM Firmware	1.3.2.8	
TPM Hierarchy	Enabled	

Power Button	Enabled	

Dell Setup and System Password

- Doesn’t seem to be a way to remove password
- But you can set it to something else
- Then you can go into setup and clear it
- Even though no hash shows up system has a password set

Dell Setup and Admin Password



BIOS Configuration (JID_040326442260)

Current Status	Task in Progress
Task Time Limit	19 mins
Elapsed Time	00:06
Task	1 of 1
Total Elapsed Time	00:00:06

Tasks are running normally.

Do not restart, press CTRL+ALT+DEL, or turn off the server. The system will restart automatically if required.