Subject: RMF Report **Date**: May 7th, 2025
Tools Used: Nessus, STIG Viewer, eMASS **Prepared By:** Jordan C. Lanning
Capture Date: May 7th, 2025

EXECUTIVE SUMMARY:

Routine scan via Nessus was conducted and reviewed via the eMASS dashboard. The analyst reviewed STIG View 3.5.1 to identify applicable misconfiguration in alignment with the organization's security requirements. Analyst assigned workflow to appropriate parties. Below are the new misconfiguration according to the organization's STIGs. POA&Ms have been created and assigned to appropriate personnel. Full STIGs are included in the corresponding tabs following the assessment.

Case (1) :

What: New workstation possess Administrator rights
Who: SGT *redacted*, Recruiter
Where: Leavenworth, KS
When: May 5th, 2025
Why: Workstation was a lateral transfer from a different unit. Device was not fully clear from receiving unit prior to local user's handling.

STIG ID: V-220712
Severity: CAT I

Remediation: Systems Administration Team will coordinate with Leavenworth (Kansas) Recruiting Unit to configure local user settings appropriately.
Completion Date: NLT May 10th, 2025, by end of business or before.

Reference: Page #3

Case (2):

What: PowerShell 2.0 Enabled
Who: LTC *redacted*, Battalion Commander
Where: Fort Drum, NY
When: April 2nd, 2025
Why: Newly published STIG of the PowerShell 2.0 which identified privilege escalations vulnerabilities when ran as an administrator.

STIG ID: V-220728
Severity: CAT II

Remediation: Systems Administration Team will disable PowerShell 2.0 and update PowerShell to the latest version. Team will coordinate with LTC *redacted* to find a time that does not conflict with his duties.
Completion Date: NLT May 10th, 2025, by end of business or before.

Reference: Page #5

Case (3):

What: Government iPhone used for official business

Subject: RMF Report **Date**: May 7th, 2025
Tools Used: Nessus, STIG Viewer, eMASS **Prepared By:** Jordan C. Lanning
Capture Date: May 7th, 2025

Who: CPT *redacted*, Company Commander
Where: Fort Jackson, SC
When: May 5th, 2025
Why: MDM on user's device was not configured to monitor the photo application on Apple iOS 17.

STIG ID: V-258355
Severity: CAT II

Remediation: CPT *redacted* will turn in government issued iPhone for configuration to Systems Administration Team and will be issued another available iPhone. If there is no other phones available, CPT *redacted* will be authorized to use personal phone for official use of non-sensitive information.
Completion Date: NLT May 7th, 2025, by end of business or before, to retrieve the misconfigured device from CPT Walker.

Reference: Page #8

OVERVIEW

STIG ID	Severity	Affected System	Assigned To	Due Date	Status
V-220712	CAT I	Workstation – Leavenworth	SysAdmin Team	May 10	Open
V-220728	CAT II	LTC Smith's Laptop	SysAdmin Team	May 10	Open
V-258355	CAT II	iPhone (Fort Jackson)	SysAdmin Team	May 7	Open

CONCLUSION

All parties have been notified of necessary actions via email and security team has received acknowledge me. The security team will continue tracking POA&M items and receive validation reports from System Administrators.

There is **no substantial threat** to the organization at this time.

If there are any additional questions or concerns, please refer them Jordan C. Lanning, at 555-555-5555 or jordanlanning@email.com. I will assist where I can.

Jordan C. Lanning, MPA, CySA+
Cybersecurity Analyst
555-555-5555

CASE (1)

Microsoft Windows 10
Version: 3 Release: 4 Benchmark Date: 02 Apr 2025

GROUP ID:
V-220712

RULE ID:
SV-220712r958726

STIG ID:
WN10-00-000070

SRG ID:
SRG-OS-000324-GPOS-00125

SEVERITY:
CAT I

LEGACY IDS:
SV-77851, V-63361

CLASSIFICATION
Unclassified

Rule Title:

Only accounts responsible for the administration of a system must have Administrator rights on the system.

Discussion:

An account that does not have Administrator duties must not have Administrator rights. Such rights would allow the account to bypass or modify required security restrictions on that machine and make it vulnerable to attack. System administrators must log on to systems only using accounts with the minimum level of authority necessary. For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group (see V-36434 in the Active Directory Domain STIG). Restricting highly privileged accounts from the local Administrators group helps mitigate the risk of privilege escalation resulting from credential theft attacks. Standard user accounts must not be members of the local administrators group.

Check Text:

```
Run "Computer Management".

Navigate to System Tools >> Local Users and Groups >> Groups.

Review the members of the Administrators group.

Only the appropriate administrator groups or accounts responsible for administration of the
system may be members of the group.
```

For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group.

Standard user accounts must not be members of the local administrator group.

If prohibited accounts are members of the local administrators group, this is a finding.

The built-in Administrator account or other required administrative accounts would not be a finding.

Fix Text:

Configure the system to include only administrator groups or accounts that are responsible for the system in the local Administrators group.

For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group.

Remove any standard user accounts.

References

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

CASE (2)

Microsoft Windows 10

Version: 3 Release: 4 Benchmark Date: 02 Apr 2025

GROUP ID:
V-220728

RULE ID:
SV-220728r958478

STIG ID:
WN10-00-000155

SRG ID:
SRG-OS-000095-GPOS-00049

SEVERITY:
CAT II

LEGACY IDS:
V-70637, SV-85259

CLASSIFICATION
Unclassified

Rule Title:

The Windows PowerShell 2.0 feature must be disabled on the system.

Discussion:

Windows PowerShell 5.0 added advanced logging features which can provide additional detail when malware has been run on a system. Disabling the Windows PowerShell 2.0 mitigates against a downgrade attack that evades the Windows PowerShell 5.0 script block logging feature.

Check Text:

```
Run "Windows PowerShell" with elevated privileges (run as administrator).


Enter the following:

Get-WindowsOptionalFeature -Online | Where FeatureName -like *PowerShellv2*


If either of the following have a "State" of "Enabled", this is a finding.


FeatureName : MicrosoftWindowsPowerShellV2

State : Enabled
```

FeatureName : MicrosoftWindowsPowerShellV2Root

State : Enabled

Alternately:

Search for "Features".

Select "Turn Windows features on or off".

If "Windows PowerShell 2.0" (whether the subcategory of "Windows PowerShell 2.0 Engine" is selected or not) is selected, this is a finding.

Fix Text:

Disable "Windows PowerShell 2.0" on the system.

Run "Windows PowerShell" with elevated privileges (run as administrator).

Enter the following:

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root

This command should disable both "MicrosoftWindowsPowerShellV2Root" and "MicrosoftWindowsPowerShellV2" which correspond to "Windows PowerShell 2.0" and "Windows PowerShell 2.0 Engine" respectively in "Turn Windows features on or off".

Alternately:

Search for "Features".

Select "Turn Windows features on or off".

De-select "Windows PowerShell 2.0".

References

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

CASE (3)

Apple iOS/iPadOS 17
Version: 2 Release: 1 Benchmark Date: 24 Jul 2024

GROUP ID:
V-258355

RULE ID:
SV-258355r959010

STIG ID:
AIOS-17-012000

SRG ID:
PP-MDF-993300

SEVERITY:
CAT II

CLASSIFICATION
Unclassified

Rule Title:

A managed photo app must be used to take and store work-related photos.

Discussion:

The iOS Photos app is unmanaged and may sync photos with a device user's personal iCloud account. Therefore, work-related photos must not be taken via the iOS camera app or stored in the Photos app. A managed photo app must be used to take and manage work-related photos. SFR ID: NA

Check Text:

```
Review configuration settings to confirm a managed photos app is installed on the iOS device.



This check procedure is performed on the iPhone and iPad.



On the iPhone and iPad:

1. Open the Settings app.

2. Tap "General".

3. Tap "VPN & Device Management".

4. Tap the DOD Configuration Profile from the Apple iOS/iPadOS management tool.

5. Tap "Apps".
```

```
6. Verify a photo capture and management app is listed.



If a managed photo capture and management app is not installed on the iPhone and iPad, this is

a finding.
```

Fix Text:

```
Install a managed photos app to take and manage work-related photos.
```

References

CCI-000097

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined restrictions.

- NIST SP 800-53 :: AC-20 (2)
- NIST SP 800-53A :: AC-20 (2).1
- NIST SP 800-53 Revision 4 :: AC-20 (2)
- NIST SP 800-53 Revision 5 :: AC-20 (2)