

CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: RUTTALA DEEPAK KUMAR

Date: 2/22/2024

Client: Momen Corporation

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to Momen Corporation to evaluate their security posture and identify potential vulnerabilities. This report provides an overview of the findings and recommendations for improving the security of the systems.

Assessment Overview:

The assessment covered the following areas:

1. Windows Security Settings and Configurations
2. Patch Management
3. User Account Settings and Permissions
4. Group Policy Settings
5. Firewall Configurations
6. Common Security Vulnerabilities
7. Findings and Recommendations

1. Windows Security Settings and Configurations

- Host Information:

- The system runs Windows 11 (Version 10.0.2200).
- Administrator rights are required for more accurate results.

- Recommendations:

- **Administrator Access:** Obtain Administrator rights for comprehensive security checks, as some checks might not succeed without it.

- **Security Configurations Review:** Review and adjust security configurations based on findings for improved system hardening.

2. Patch Management:

- Findings:

- The system appears up-to-date with 6 installed hotfixes.

- Recommendations:

- **Ongoing Monitoring:** Continue regular monitoring and updating to maintain patch compliance, ensuring the system is protected against known vulnerabilities.

3. User Account Settings and Permissions:

- **Findings:**

- More than one account is in the local Administrators group.

- **Recommendations:**

- **Local Administrator Accounts:** Review and secure local Administrator accounts to prevent unauthorized access and privilege escalation.

4. Group Policy Settings:

- **Findings:**

- GPOs (Group Policy Objects) may not be assigned to the system.

- **Recommendations:**

- **GPO Assignment:** Investigate and address any issues with GPO assignment to ensure consistent security policy application across the system.

5. Firewall Configurations:

- **Findings:**

- WinRM Firewall rules for remote connections are disabled.

- Recommendations:

- WinRM Configuration: Review and configure WinRM Firewall rules for secure remote connections, enhancing the overall system security posture.

6. Common Security Vulnerabilities:

- Findings:

- AppLocker is not configured.

- LAPS (Local Administrator Password Solution) is not installed.

- SMBv1 is enabled.

- Recommendations:

- AppLocker Implementation: Consider implementing AppLocker for application control, preventing unauthorized software execution.

- LAPS Installation: Investigate the installation of LAPS for managing local administrator passwords securely.

- SMBv1 Disabling: Disable SMBv1 to mitigate the risk associated with this outdated and vulnerable protocol.

General Recommendations:

- **Administrator Rights:** Ensure Administrator rights are obtained for more comprehensive security checks, addressing issues that require elevated privileges.
- **Ongoing Patch Management:** Regularly monitor and update the system for the latest security patches to mitigate potential vulnerabilities.
- **Event Log Size Adjustment:** Review and adjust event log sizes to accommodate log data and facilitate effective security monitoring.
- **PowerShell Version 2 Support:** Consider disabling PowerShell version 2 support if not needed, reducing the attack surface.
- **Remote Access Security:** Implement security best practices for remote access configurations to protect against unauthorized access.
- **Additional Security Measures:** Address other identified security issues based on organizational policies, ensuring a holistic approach to system security.

There is Screenshots :

1- DESKTOP-T0OC4AH-chaps

```
DESKTOP-T0OC4AH-chaps - Notepad
File Edit Format View Help
[*] Start Date/Time: 29240222T1204461410Z
[ ] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to separate file\n
[*] Windows Version: Microsoft Windows NT 10.0.19044.2
[*] Windows Default Path for momen : C:\Windows\System32\;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\momen\AppData\Local\Win
[*] Host network interface assigned: 192.168.1.2
[*] Checking IPv6 Network Settings
[ ] Host IPv6 network interface assigned (gwmi): fe80::cdc8:8a10:7844:b41c
[*] Checking Windows AutoUpdate Configuration
[*] Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4
[*] Checking for missing Windows patches with Critical or Important Microsoft Security values. NOTE: This may take a few minutes.
[*] Windows system appears to be up-to-date for critical and important patches.
[*] Checking BitLocker Encryption
[*] BitLocker not detected. Please check for other encryption methods.
[*] Checking if users can install software as NT AUTHORITY\SYSTEM
[ ] Users cannot install software as NT AUTHORITY\SYSTEM
[*] Testing if PowerShell Commandline Auditing is Enabled
[ ] ProcessCreationIncludeCommandLine_Enabled is Not Set
[*] Testing if PowerShell Module Logging is Enabled
[ ] EnableModuleLogging is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[ ] EnableScriptBlockLogging is Not Set
[*] Testing if PowerShell EnableScriptBlockInvocationLogging is Enabled
[ ] EnableScriptBlockInvocationLogging is Not Set
[*] Testing if PowerShell EnableTranscripting is Enabled
[ ] EnableTranscripting is Not Set
[*] Testing if PowerShell EnableInvocationHeader is Enabled
[ ] EnableInvocationHeader is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[ ] EnableProtectedEventLogging is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[*] Testing Microsoft-Windows-SMBServer/Audit log size failed.
[*] Testing Security log size failed.
[ ] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operational] GB: 0.015 GB
[ ] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/Operational] GB: 0.01 GB
[ ] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB: 0.001 GB
[ ] Microsoft-Windows-Security-Mitigation/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Security-Mitigation/Operational] GB: 0.001 GB
[ ] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.001 GB
[ ] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[ ] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
Ln 1, Col 1 100% Windows (CRLF) UTF-16 LE
Type here to search 18°C مئتمنى جوتة 1:11 PM 2/22/2024
```

2.SKTOP-T0OC4AH-sysinfo

```
USKTOP-T0OC4AH-sysinfo - Notepad
File Edit Format View Help
Host Name: DESKTOP-T0OC4AH
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19044 N/A Build 19044
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: momen
Registered Organization:
Product ID: 00330-80000-00000-AA538
Original Install Date: 9/1/2023, 2:03:45 AM
System Boot Time: 2/22/2024, 11:28:56 AM
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: AMD64 Family 23 Model 24 Stepping 1 AuthenticAMD ~2096 Mhz
BIOS Version: Phoenix Technologies LTD 6.00, 7/29/2019
Windows Directory: C:\Windows
System Directory: C:\Windows\System32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC+02:00) Cairo
Total Physical Memory: 4,095 MB
Available Physical Memory: 1,620 MB
Virtual Memory: Max Size: 5,503 MB
Virtual Memory: Available: 2,321 MB
Virtual Memory: In Use: 3,182 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\DESKTOP-T0OC4AH
netfix(s): 6 netfix(s) Installed.
[01]: KB902122
[02]: KB9005791
[03]: KB9020583
[04]: KB9026037
[05]: KB9006670
[06]: KB9005899
Network Card(s): 1 NIC(s) Installed.
```

