Amazon Inspector - Assessment Report

Findings Report

Report generated on 2018-02-08 at 04:53:11 UTC

Assessment Template: mgc-test-template

Assessment Run start: 2018-02-08 at 03:39:14 UTC
Assessment Run end: 2018-02-08 at 04:42:47 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2018-02-08 03:39:14 UTC for assessment template 'mgc-test-template'. The assessment target included 1 instances, and was tested against 4 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
aws:cloudformation:stack-name	mgc-sec-test-2

The following Rules Packages were assessed. A total of 753 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
CIS Operating System Security Configuration Benchmarks-1.0	736	0	0	0
Common Vulnerabilities and Exposures-1.1	4	9	1	0
Runtime Behavior Analysis-1.0	0	0	1	2
Security Best Practices-1.0	0	0	0	0

Section 2: What is Tested

This section details the Rules Packages included in this assessment run, and the EC2 instances included in the assessment target.

2.1: Rules Packages - Count: 4

2.1.1: CIS Operating System Security Configuration Benchmarks-1.0

Description: The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security.

The rules in this package help establish a secure configuration posture for the following operating systems:

- Amazon Linux version 2015.03 (CIS benchmark v1.1.0)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)

If a particular CIS benchmark appears in a finding produced by an Amazon Inspector assessment run, you can download a detailed PDF description of the benchmark from https://benchmarks.cisecurity.org/ (free registration

required). The benchmark document provides detailed information about this CIS benchmark, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.1.2: Common Vulnerabilities and Exposures-1.1

Description: The rules in this package help verify whether the EC2 instances in your application are exposed to Common Vulnerabilities and Exposures (CVEs). Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference for publicly known information security vulnerabilities and exposures. For more information, see https://cve.mitre.org/. If a particular CVE appears in one of the produced Findings at the end of a completed Inspector assessment, you can search https://cve.mitre.org/ using the CVE's ID (for example, "CVE-2009-0021") to find detailed information about this CVE, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.3: Runtime Behavior Analysis-1.0

Description: These rules analyze the behavior of your instances during an assessment run, and provide guidance on how to make your instances more secure.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.1.4: Security Best Practices-1.0

Description: The rules in this package help determine whether your systems are configured securely.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.2: Assessment Target - mgc-test-template

2.2.1: EC2 Tags:

The following EC2 tags (Key/Value pairs) were used to define this assessment target.

Key	Value
aws:cloudformation:stack-name	mgc-sec-test-2

2.2.2: Instances - Count 1

Instance ID
i-03e085d4f68678768

Section 3: Findings Summary

This section lists the rules that generated findings, the severity of the finding, and the number of instances affected. More details about the findings can be found in the "Findings Details" section. Rules that passed on all target instances available during the assessment run are listed in the "Passed Rules" section.

3.1: Findings table - CIS Operating System Security Configuration Benchmarks-1.0

3.1.1 Level 1 - Domain Controller

Rule	Severity	Failed
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	High	1
1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	High	1
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	High	1
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	High	1
2.2.2 (L1) Configure 'Access this computer from the network'	High	1
2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.6 (L1) Configure 'Allow log on locally'	High	1
2.2.7 (L1) Configure 'Allow log on through Remote Desktop Services'	High	1
2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	High	1
2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	High	1
2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'	High	1
2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'	High	1
2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	High	1
2.2.25 (L1) Configure 'Impersonate a client after authentication'	High	1
2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	High	1
2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'	High	1

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'	High	1
2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	High	1
2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	High	1
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	High	1
2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	High	1
2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)	High	1
2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)	High	1
2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)	High	1
2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	High	1
2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	High	1
2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	High	1
2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	High	1
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	High	1
2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	High	1
2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	High	1
2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	High	1
2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously'	High	1
2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	High	1
2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	High	1
2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	High	1
2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	High	1

2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	High	1
2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	High	1
2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'	High	1
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	High	1
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	High	1
2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	High	1
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	High	1
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	High	1
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	High	1
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	High	1
9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	High	1
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	High	1
9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	High	1
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	High	1
9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	High	1

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	High	1
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	High	1
9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	High	1
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	High	1
9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	High	1
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	High	1
9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	High	1
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	High	1
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'	High	1
9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	High	1
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	High	1
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	High	1
9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	High	1
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	High	1
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	High	1
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	High	1
17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	High	1
17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only)	High	1

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'	High	1
17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'	High	1
17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	High	1
17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'	High	1
17.4.1 (L1) Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only)	High	1
17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only)	High	1
17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	High	1
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	High	1
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	High	1
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	High	1
17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'	High	1
18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	High	1
18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	High	1
18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	High	1
18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	High	1
18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	High	1
18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	High	1
18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	High	1
18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	High	1

18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	High	1
18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	High	1
18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'	High	1
18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'	High	1
18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	High	1
18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	High	1
18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	High	1
18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	High	1
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	High	1
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	High	1
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	High	1
18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	High	1
18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	High	1
18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'	High	1
18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'	High	1
18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed	High	1
18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)	High	1
18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	High	1
18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'	High	1
18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'	High	1
18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'	High	1
18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'	High	1

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	High	1
18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	High	1
18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	High	1
18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	High	1
18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	High	1
18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	High	1
18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	High	1
18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	High	1
18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	High	1
18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	High	1
18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	High	1
18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	High	1
18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	1
18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'	High	1
18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	High	1
18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	High	1

18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	High	1
18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	High	1
18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	High	1
18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	High	1
18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	High	1
18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	High	1
18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	High	1
18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'	High	1

3.1.2 Level 1 - Member Server

Rule	Severity	Failed
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	High	1
1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	High	1
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	High	1
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	High	1
2.2.2 (L1) Configure 'Access this computer from the network'	High	1
2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.6 (L1) Configure 'Allow log on locally'	High	1
2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	High	1
2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	High	1
2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'	High	1
2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'	High	1

2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	High	1
2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	High	1
2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'	High	1
2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'	High	1
2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	High	1
2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	High	1
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	High	1
2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	High	1
2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	High	1
2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	High	1
2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	High	1
2.3.7.7 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	High	1
2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	High	1
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	High	1
2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	High	1
2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	High	1
2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	High	1
2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	High	1
2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	High	1
2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	High	1

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	High	1
2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	High	1
2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	High	1
2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'	High	1
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	High	1
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	High	1
2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	High	1
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	High	1
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	High	1
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	High	1
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	High	1
9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	High	1
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	High	1
9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	High	1
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	High	1

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	High	1
9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	High	1
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	High	1
9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	High	1
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	High	1
9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	High	1
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	High	1
9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	High	1
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	High	1
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'	High	1
9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	High	1
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	High	1
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	High	1
9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	High	1
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	High	1
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	High	1
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	High	1
17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	High	1

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'	High	1
17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'	High	1
17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	High	1
17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'	High	1
17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	High	1
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	High	1
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	High	1
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	High	1
17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'	High	1
18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	High	1
18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	High	1
18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	High	1
18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	High	1
18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)	High	1
18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)	High	1
18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	High	1
18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	High	1
18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	High	1
18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	High	1

18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	High	1
18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	High	1
18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	High	1
18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	High	1
18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	High	1
18.6.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)	High	1
18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	High	1
18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'	High	1
18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'	High	1
18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	High	1
18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	High	1
18.8.24.1 (L1) Ensure 'Always use classic logon' is set to 'Enabled'	High	1
18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	High	1
18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	High	1
18.8.31.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	High	1
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	High	1
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	High	1
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	High	1
18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	High	1
18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	High	1
18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'	High	1
18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'	High	1
18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed	High	1

18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)	High	1
18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	High	1
18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'	High	1
18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'	High	1
18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'	High	1
18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	High	1
18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	High	1
18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	High	1
18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	High	1
18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	High	1
18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	High	1
18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	High	1
18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	High	1

18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	High	1
18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	High	1
18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	High	1
18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	High	1
18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	1
18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'	High	1
18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	High	1
18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	High	1
18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	High	1
18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	High	1
18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	High	1
18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	High	1
18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	High	1
18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	High	1
18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	High	1
18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'	High	1

3.1.3 Level 2 - Domain Controller

Rule	Severity	Failed
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	High	1

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	High	1
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	High	1
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	High	1
2.2.2 (L1) Configure 'Access this computer from the network'	High	1
2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.6 (L1) Configure 'Allow log on locally'	High	1
2.2.7 (L1) Configure 'Allow log on through Remote Desktop Services'	High	1
2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	High	1
2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	High	1
2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'	High	1
2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'	High	1
2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	High	1
2.2.25 (L1) Configure 'Impersonate a client after authentication'	High	1
2.2.29 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only)	High	1
2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	High	1
2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'	High	1
2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'	High	1
2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	High	1
2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	High	1
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	High	1
2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	High	1
2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)	High	1
2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)	High	1
2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)	High	1
2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	High	1
2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	High	1

2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	High	1
2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	High	1
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	High	1
2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	High	1
2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	High	1
2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	High	1
2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	High	1
2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously'	High	1
2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	High	1
2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	High	1
2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	High	1
2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	High	1
2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	High	1
2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	High	1
2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'	High	1
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	High	1
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	High	1

2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	High	1
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	High	1
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	High	1
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	High	1
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	High	1
9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	High	1
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	High	1
9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	High	1
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	High	1
9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	High	1
9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	High	1
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	High	1
9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	High	1
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	High	1
9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	High	1
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	High	1

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	High	1
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	High	1
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'	High	1
9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	High	1
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	High	1
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	High	1
9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	High	1
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	High	1
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	High	1
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	High	1
17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	High	1
17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only)	High	1
17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'	High	1
17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'	High	1
17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	High	1
17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'	High	1
17.4.1 (L1) Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only)	High	1
17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only)	High	1
17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	High	1
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	High	1
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	High	1
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	High	1

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'	High	1
18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	High	1
18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	High	1
18.3.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'	High	1
18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	High	1
18.3.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'	High	1
18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	High	1
18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	High	1
18.3.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	High	1
18.3.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	High	1
18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	High	1
18.4.8.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'	High	1
18.4.8.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	High	1
18.4.9.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'	High	1
18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	High	1
18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	High	1
18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	High	1

18.4.18.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')	High	1
18.4.19.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'	High	1
18.4.19.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'	High	1
18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	High	1
18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'	High	1
18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'	High	1
18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	High	1
18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	High	1
18.8.19.1.1 (L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	High	1
18.8.19.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'	High	1
18.8.19.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'	High	1
18.8.19.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'	High	1
18.8.19.1.5 (L2) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	High	1
18.8.19.1.6 (L2) Ensure 'Turn off Internet File Association service' is set to 'Enabled'	High	1
18.8.19.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled'	High	1
18.8.19.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'	High	1
18.8.19.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'	High	1
18.8.19.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'	High	1
18.8.19.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'	High	1
18.8.19.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'	High	1
18.8.19.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'	High	1
18.8.19.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	High	1
18.8.28.4.1 (L2) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	High	1

18.8.28.4.2 (L2) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	High	1
18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	High	1
18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	High	1
18.8.38.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'	High	1
18.8.38.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'	High	1
18.8.43.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled'	High	1
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	High	1
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	High	1
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	High	1
18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	High	1
18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	High	1
18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'	High	1
18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'	High	1
18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed	High	1
18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)	High	1
18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	High	1
18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'	High	1
18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'	High	1
18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'	High	1
18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1

18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	High	1
18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	High	1
18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	High	1
18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	High	1
18.9.35.1 (L2) Ensure 'Turn off location' is set to 'Enabled'	High	1
18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	High	1
18.9.48.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'	High	1
18.9.48.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled'	High	1
18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	High	1
18.9.48.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled'	High	1
18.9.48.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'	High	1
18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	High	1
18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	High	1
18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	High	1
18.9.48.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'	High	1
18.9.48.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'	High	1
18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	High	1
18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	High	1
18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	High	1

18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	1
18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'	High	1
18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	High	1
18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	High	1
18.9.69.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'	High	1
18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	High	1
18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	High	1
18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	High	1
18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	High	1
18.9.82.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled'	High	1
18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	High	1
18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	High	1
18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	High	1
18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'	High	1

3.1.4 Level 2 - Member Server

Rule	Severity	Failed
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	High	1
1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	High	1
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	High	1
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	High	1

2.2.2 (L1) Configure 'Access this computer from the network'	High	1
2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.6 (L1) Configure 'Allow log on locally'	High	1
2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	High	1
2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	High	1
2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'	High	1
2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'	High	1
2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	High	1
2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	High	1
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	High	1
2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'	High	1
2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'	High	1
2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	High	1
2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	High	1
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	High	1
2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	High	1
2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	High	1
2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	High	1
2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	High	1
2.3.7.5 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only)	High	1
2.3.7.7 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	High	1
2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	High	1
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	High	1
2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	High	1
2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	High	1

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	High	1
2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	High	1
2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	High	1
2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	High	1
2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	High	1
2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	High	1
2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	High	1
2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	High	1
2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	High	1
2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	High	1
2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'	High	1
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	High	1
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	High	1
2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	High	1
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	High	1
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	High	1
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	High	1
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	High	1
9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	High	1
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	High	1
9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	High	1
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	High	1
9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	High	1
9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	High	1
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	High	1
9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'	High	1
9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'	High	1
9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	High	1
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	High	1
9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	High	1
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	High	1
9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	High	1
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	High	1
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'	High	1
9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	High	1
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	High	1
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	High	1

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	High	1
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	High	1
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	High	1
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	High	1
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	High	1
17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	High	1
17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'	High	1
17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'	High	1
17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	High	1
17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'	High	1
17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	High	1
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	High	1
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	High	1
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	High	1
17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'	High	1
18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	High	1
18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	High	1
18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	High	1
18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	High	1
18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)	High	1
18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)	High	1
18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	High	1

18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	High	1
18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	High	1
18.3.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'	High	1
18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	High	1
18.3.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'	High	1
18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	High	1
18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	High	1
18.3.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	High	1
18.3.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	High	1
18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	High	1
18.4.8.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'	High	1
18.4.8.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	High	1
18.4.9.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'	High	1
18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	High	1
18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	High	1
18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	High	1
18.4.18.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')	High	1
18.4.19.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'	High	1

18.4.19.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'	High	1
18.6.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)	High	1
18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	High	1
18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'	High	1
18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'	High	1
18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	High	1
18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	High	1
18.8.19.1.1 (L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	High	1
18.8.19.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'	High	1
18.8.19.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'	High	1
18.8.19.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'	High	1
18.8.19.1.5 (L2) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	High	1
18.8.19.1.6 (L2) Ensure 'Turn off Internet File Association service' is set to 'Enabled'	High	1
18.8.19.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled'	High	1
18.8.19.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'	High	1
18.8.19.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'	High	1
18.8.19.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'	High	1
18.8.19.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'	High	1
18.8.19.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'	High	1
18.8.19.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'	High	1
18.8.19.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	High	1
18.8.24.1 (L1) Ensure 'Always use classic logon' is set to 'Enabled'	High	1
18.8.28.4.1 (L2) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	High	1

18.8.28.4.2 (L2) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	High	1
18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	High	1
18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	High	1
18.8.31.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	High	1
18.8.31.2 (L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only)	High	1
18.8.38.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'	High	1
18.8.38.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'	High	1
18.8.43.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled'	High	1
18.8.43.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only)	High	1
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	High	1
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	High	1
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	High	1
18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	High	1
18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	High	1
18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'	High	1
18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'	High	1
18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed	High	1
18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)	High	1
18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	High	1
18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'	High	1
18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'	High	1
18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'	High	1
18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'	High	1
18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'	High	1

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	High	1
18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	High	1
18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	High	1
18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	High	1
18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	High	1
18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	High	1
18.9.35.1 (L2) Ensure 'Turn off location' is set to 'Enabled'	High	1
18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	High	1
18.9.48.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'	High	1
18.9.48.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled'	High	1
18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	High	1
18.9.48.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled'	High	1
18.9.48.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'	High	1
18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	High	1
18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	High	1
18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	High	1
18.9.48.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'	High	1
18.9.48.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'	High	1

18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	High	1
18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	High	1
18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	High	1
18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	1
18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'	High	1
18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	High	1
18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	High	1
18.9.69.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'	High	1
18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	High	1
18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	High	1
18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	High	1
18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	High	1
18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	High	1
18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	High	1
18.9.82.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled'	High	1
18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	High	1
18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	High	1
18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'	High	1
18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	High	1
18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'	High	1

3.2: Findings table - Common Vulnerabilities and Exposures-1.1

Rule	Severity	Failed
CVE-2012-2531	Medium	1
CVE-2012-2532	High	1
CVE-2017-5715	Medium	1
CVE-2017-5753	Medium	1
CVE-2017-5754	Medium	1
CVE-2018-0741	Medium	1
CVE-2018-0747	Low	1
CVE-2018-0748	Medium	1
CVE-2018-0749	Medium	1
CVE-2018-0750	Medium	1
CVE-2018-0754	Medium	1
CVE-2018-0762	High	1
CVE-2018-0772	High	1
CVE-2018-0788	High	1

3.3: Findings table - Runtime Behavior Analysis-1.0

Rule	Severity	Failed
Insecure client protocols (general)	Low	1
Insecure server protocols	Informational	1
Unused listening TCP ports	Informational	1

3.4: Findings table - Security Best Practices-1.0

No findings were generated for this rules package.

Section 4: Findings Details

This section details the findings generated in this assessment run, and the instances that generated the finding. If an instance is not listed here, that means it was checked and passed.

4.1: Findings details - CIS Operating System Security Configuration Benchmarks-1.0

4.1.1 Level 1 - Domain Controller

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Severity
High

Description
Description This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s). Rationale The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Recommendation

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Failed Instances
i-03e085d4f68678768

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'

Severity
High

Description
Description This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s). Rationale Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings \Account Policies\Password Policy\Minimum password age Impact: If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Failed Instances
i-03e085d4f68678768

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Severity
High

Description
Description This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Rationale Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or

lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Failed Instances
i-03e085d4f68678768

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Severity
High

Description
Description This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0. Rationale Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Failed Instances
i-03e085d4f68678768

2.2.2 (L1) Configure 'Access this computer from the network'

Severity
High

Description
Description This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators, Authenticated Users. Rationale Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Access this computer from the network Impact: If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore it is recommended that it is assigned to the Users group. If you have installed optional components such as ASP.NET or

Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Failed Instances
i-03e085d4f68678768

2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE: Computer Configuration \Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment \Adjust memory quotas for a process Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Failed Instances

i-03e085d4f68678768

2.2.6 (L1) Configure 'Allow log on locally'

Severity
High

Description
Description This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT +DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators. Rationale Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on locally Impact: If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

Failed Instances
i-03e085d4f68678768

2.2.7 (L1) Configure 'Allow log on through Remote Desktop Services'

Severity

High

Description

Description This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the restricted groups feature to ensure that no user accounts are part of the Remote Desktop Users group. Restrict this user right to the Administrators group, and possibly the Remote Desktop Users group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: Administrators, Remote Desktop Users. Note: A server that holds the Remote Desktop Services Role with Remote Desktop Connection Broker Role Service will require a special exception to this recommendation, to allow the Authenticated Users group to be granted this user right. Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass. Rationale Any account with the Allow log on through Terminal Services user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on through Remote Desktop Services Impact: Removal of the Allow log on through Terminal Services user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances

i-03e085d4f68678768

2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'

Severity

High

Description
Description This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators. Rationale Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Back up files and directories Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Failed Instances
i-03e085d4f68678768

2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'

Severity
High

Description
Description This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests. Rationale Accounts that have the Deny log on

as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a batch job Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Failed Instances
i-03e085d4f68678768

2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'

Severity
High

Description
Description This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests. Note: This security setting does not apply to the System, Local Service, or Network Service accounts. Rationale Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a service Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Failed Instances
i-03e085d4f68678768

2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'

Severity
High

Description
Description This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests. Rationale Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on locally Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Severity
High

Description
Description This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account. Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server. Rationale Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests, Local account: Computer Configuration\Policies\Windows Settings \Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Failed Instances
i-03e085d4f68678768

2.2.25 (L1) Configure 'Impersonate a client after authentication'

Severity
High

Description
Description The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect#x2014;for example, by remote

procedure call (RPC) or named pipes#x2014;to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels. Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started. Also, a user can impersonate an access token if any of the following conditions exist:- The access token that is being impersonated is for this user.- The user, in this logon session, logged on to the network with explicit credentials to create the access token.- The requested level is less than Impersonate, such as Anonymous or Identify. An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE .Level 1 - Member Server. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS. Rationale An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Impersonate a client after authentication Impact: In most cases this configuration will have no impact. If you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to also assign the user right to IIS_IUSRS.

Failed Instances
i-03e085d4f68678768

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description

Description This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

Recommendation

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Failed Instances

i-03e085d4f68678768

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Severity

High

Description

Description This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. Rationale An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data

that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Failed Instances
i-03e085d4f68678768

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators. Rationale The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain

functionality, such as processing logons for new passwords#x2014;the Primary Domain Controller (PDC) Emulator role.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Shut down the system Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled. Rationale In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Failed Instances
i-03e085d4f68678768

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'

Severity
High

Description
Description The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). Rationale The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies

\Security Options\Accounts: Rename administrator account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Failed Instances
i-03e085d4f68678768

2.3.1.5 (L1) Configure 'Accounts: Rename guest account'

Severity
High

Description
Description The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. Rationale The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

Failed Instances
i-03e085d4f68678768

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in

Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled. Rationale Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Failed Instances
i-03e085d4f68678768

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized

users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators. Rationale Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default value. Only Administrators will be able to format and eject removable NTFS media.

Failed Instances
i-03e085d4f68678768

2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)

Severity
High

Description
Description This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job. Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu. The recommended state for this setting is: Disabled. Rationale If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform

tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks Impact: The impact should be small for most organizations. Users (including those in the Server Operators group) will still be able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Failed Instances
i-03e085d4f68678768

2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)

Severity
High

Description
Description This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. The recommended state for this setting is: Require signing. Rationale Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Require signing: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Domain controller: LDAP server signing requirements

Impact: Clients that do not support LDAP signing will be unable to run LDAP queries against the domain controllers. All Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see Microsoft Knowledge Base article 325465: Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools. Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Failed Instances
i-03e085d4f68678768

2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)

Severity
High

Description
Description This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password.Default: This policy is not defined, which means that the system treats it as Disabled. The recommended state for this setting is: Disabled. Rationale If you enable this policy setting on all domain controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes Impact: None. This is the default configuration.

Failed Instances

i-03e085d4f68678768

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled. Rationale An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

Failed Instances
i-03e085d4f68678768

2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'

Severity
High

Description
Description This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce

corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons#x2014;for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Recommendation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message text for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances
i-03e085d4f68678768

2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'

Severity
High

Description
Description This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It

may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Recommendation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message title for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances
i-03e085d4f68678768

2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Severity
High

Description
Description This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark. Rationale Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is

removed to ensure that only the user with the smart card is accessing resources using those credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior Impact: If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Failed Instances
i-03e085d4f68678768

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally

sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances

i-03e085d4f68678768

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications,

older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Severity
High

Description
Description This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis

for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms with the benchmark. Rationale The identity of a computer can be spoofed to gain unauthorized access to network resources.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms with the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Microsoft network server: Server SPN target name validation level Impact: All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Failed Instances
i-03e085d4f68678768

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: Disabled. Rationale If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003-based domains. For example, the following computers may not work:Windows NT 4.0-based Remote Access Service servers.Microsoft SQL Servers#x2122; that run on Windows NT 3.x-based or Windows NT 4.0-based computers.Remote Access Service or Microsoft SQL servers that run on Windows 2000-based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Failed Instances
i-03e085d4f68678768

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting is: Enabled. Rationale An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares Impact: It will be impossible to grant access to users of

another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Failed Instances
i-03e085d4f68678768

2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously'

Severity
High

Description
Description This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. The recommended state for this setting is: Level 1 - Domain Controller. The recommended state for this setting is: LSARPC, NETLOGON, SAMR and (when the legacy Computer Browser service is enabled) BROWSER.Level 1 - Member Server. The recommended state for this setting is: <blank> (i.e. None), or (when the legacy Computer Browser service is enabled) BROWSER. Note: A server that holds the Remote Desktop Services Role with Remote Desktop Licensing Role Service will require a special exception to this recommendation, to allow the HydraLSPipe and TermServLicensing Named Pipes to be accessed anonymously. Rationale Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Network access: Named Pipes that can be accessed anonymously Impact: This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The BROWSER named pipe may need to be added to this list if the Computer Browser service is needed for supporting legacy components. The Computer Browser service is disabled by default.

Failed Instances

i-03e085d4f68678768

2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Severity
High

Description
Description This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None). Rationale It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously Impact: There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

Failed Instances
i-03e085d4f68678768

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Severity
High

Description
Description When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled. Rationale When connecting to computers running versions of Windows earlier than Windows Vista or Windows

Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM Impact: If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Failed Instances
i-03e085d4f68678768

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Severity
High

Description
Description Allow NTLM to fall back to NULL session when used with LocalSystem. The default is TRUE up to Windows Vista / Server 2008 and FALSE from Windows 7 / Server 2008 R2 and beyond. The recommended state for this setting is: Disabled. Rationale NULL sessions are less secure because by definition they are unauthenticated.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback

Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Failed Instances
i-03e085d4f68678768

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

Severity
High

Description
Description This setting determines if online identities are able to authenticate to this computer. Windows 7 and Windows Server 2008 R2 introduced an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled. Rationale The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities Impact: Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7 and later.

Failed Instances
i-03e085d4f68678768

2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Severity
High

Description
Description This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types. Rationale The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos Impact: If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Failed Instances
i-03e085d4f68678768

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

Severity
High

Description
Description LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and

network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: Join a domainAuthenticate between Active Directory forestsAuthenticate to down-level domainsAuthenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: Send LM & NTLM responsesSend LM & NTLM #x2014; use NTLMv2 session security if negotiatedSend NTLM responses onlySend NTLMv2 responses onlySend NTLMv2 responses only\refuse LMSend NTLMv2 responses only\refuse LM & NTLMNot Defined The Network security: LAN Manager authentication level setting determines which challenge/ response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send LM & NTLM - use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).These settings correspond to the levels discussed in other Microsoft documents as follows:Level 0 - Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 1 - Use NTLMv2 session security if negotiated. Clients use LM

and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 3 - Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2.Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM. Rationale In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses#x2014;the weakest form of authentication response#x2014;are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Recommendation

To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level Impact: Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain

resources by using LM and NTLM.Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Failed Instances
i-03e085d4f68678768

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has

gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Impact: Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed

through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Impact: Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'

Severity
High

Description
Description This security setting determines which subsystems can optionally be started up to support your applications. The recommended state for this setting is: Defined: (blank) Rationale Leaving POSIX enabled could introduce an additional attack surface in your environment.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Defined: (blank) : Computer Configuration\Security Settings\Local Policies\Security Options\System settings: Optional subsystems Impact: Removes POSIX compatibility.

Failed Instances
i-03e085d4f68678768

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: Enabled. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-

in Administrator account Impact: Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Failed Instances
i-03e085d4f68678768

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for administrators. The options are:- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.- Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.- Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: Prompt for consent on the secure desktop. Rationale One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of

its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Impact: This policy setting controls the behavior of the elevation prompt for administrators.

Failed Instances
i-03e085d4f68678768

2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for standard users. The options are: Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: Automatically deny elevation requests. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege

operations and requires that the user be able to supply administrative credentials in order for the program to run.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users Impact: Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Failed Instances
i-03e085d4f68678768

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances

i-03e085d4f68678768

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista / Server 2008 and above, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this

opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\domainfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\domainfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale
Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\privatefw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\privatefw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Private Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit

(KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The

recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before

deploying. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: Yes. Rationale Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows

Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No. Rationale When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Severity
High

Description

Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No. Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\publicfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Public Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it

may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon.4775: An account could not be mapped for logon.4776: The domain controller attempted to validate the credentials for an account.4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted.Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Application Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created.4742: A computer account was changed.4743: A computer account was deleted.

The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Computer Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include: 4744: A security-disabled local group was created.4745: A security-disabled local group was changed.4746: A member was added to a security-disabled local group.4747: A member was removed from a security-disabled local group.4748: A security-disabled local group was deleted.4749: A security-disabled global group was created.4750: A security-disabled global group was changed.4751: A member was added to a security-disabled global group.4752: A member was removed from a security-disabled global group.4753: A security-disabled global group was deleted.4759: A security-disabled universal group was created.4760: A security-disabled universal group was changed.4761: A member was added to a

security-disabled universal group.4762: A member was removed from a security-disabled universal group.4763: A security-disabled universal group was deleted. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may provide an organization with insight when investigating an incident. For example, when a given unauthorized user was added to a sensitive distribution group.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Distribution Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed.4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management

\Audit Other Account Management Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created.4728: A member was added to a security-enabled global group.4729: A member was removed from a security-enabled global group.4730: A security-enabled global group was deleted.4731: A security-enabled local group was created.4732: A member was added to a security-enabled local group.4733: A member was removed from a security-enabled local group.4734: A security-enabled local group was deleted.4735: A security-enabled local group was changed.4737: A security-enabled global group was changed.4754: A security-enabled universal group was created.4755: A security-enabled universal group was changed.4756: A member was added to a security-enabled universal group.4757: A member was removed from a security-enabled universal group.4758: A security-enabled universal group was deleted.4764: A group's type was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Security Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created.4722: A user account was enabled.4723: An attempt was made to change an account's password.4724: An attempt was made to reset an account's password.4725: A user account was disabled.4726: A user account was deleted.4738: A user account was changed.4740: A user account was locked out.4765: SID History was added to an account.4766: An attempt to add SID History to an account failed.4767: A user account was unlocked.4780: The ACL was set on accounts which are members of administrators groups.4781: The name of an account was changed:4794: An attempt was made to set the Directory Services Restore Mode.5376: Credential Manager credentials were backed up.5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit User Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'

Severity
High

Description
Description This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created.4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings \Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected.

Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.4.1 (L1) Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to domain controllers. Events for this subcategory include: 4662 : An operation was performed on an object. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers. Events for this subcategory include: 5136 : A directory service object was modified.5137 : A directory service object was created.5138 : A directory service object was undeleted.5139 : A directory service object was moved. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure. Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Changes Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Severity
High

Description

Description This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected.4778: A session was reconnected to a Window Station.4779: A session was disconnected from a Window Station.4800: The workstation was locked.4801: The workstation was unlocked.4802: The screen saver was invoked.4803: The screen saver was dismissed.5378: The requested credentials delegation was disallowed by policy.5632: A request was made to authenticate to a wireless network.5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances

i-03e085d4f68678768

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'

Severity

High

Description

Description This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed.4719: System audit policy was changed.4902: The Per-user audit policy table was created.4904: An attempt was made to register a security event source.4905: An

attempt was made to unregister a security event source.4906: The CrashOnAuditFail value has changed.4907: Auditing settings on object were changed.4908: Special Groups Logon table modified.4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object.

The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning

hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.5478: IPsec Services has started successfully.5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances

i-03e085d4f68678768

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'

Severity

High

Description
Description This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority.4611: A trusted logon process has been registered with the Local Security Authority.4614: A notification package has been loaded by the Security Account Manager.4622: A security package has been loaded by the Local Security Authority.4697: A service was installed in the system. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Severity
High

Description
Description This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any

network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled. Rationale If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None. By default this entry is not enabled.

Failed Instances
i-03e085d4f68678768

18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configur ation\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Severity
High

Description
Description Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled. Rationale This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Failed Instances
i-03e085d4f68678768

18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Severity
High

Description
Description NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled. Rationale The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Failed Instances
i-03e085d4f68678768

18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Severity
High

Description
Description The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the

system path first, and then search the current working folder.Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: Enabled. Rationale If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Failed Instances
i-03e085d4f68678768

18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Severity
High

Description
Description Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds. Rationale The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who

could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Failed Instances
i-03e085d4f68678768

18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Severity
High

Description
Description This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less. Rationale If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less: Computer Configuration\Policies\Administrative Templates \MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required -

it is included with Microsoft Security Compliance Manager (SCM). Impact: This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

Failed Instances
i-03e085d4f68678768

18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Severity
High

Description
Description You can use this procedure to enable or disable the user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled. Rationale Allowing users to create a network bridge increases the risk and attack surface from the bridged network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network Impact: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, you can disable the Network Bridge setting on a computer. If you disable Network Bridge on a computer, users cannot create or configure a network bridge. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

Failed Instances
i-03e085d4f68678768

18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled. Rationale Allowing regular users to set a network location increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Require domain users to elevate when setting a network's location Impact: If you enable this policy setting domain users must elevate when setting a network's location. If you disable or do not configure this policy setting domain users can set a network's location without elevating.

Failed Instances
i-03e085d4f68678768

18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Severity
High

Description
Description This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares. Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing. Rationale In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was

not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Failed Instances
i-03e085d4f68678768

18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Severity
High

Description
Description When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials

protection and management May 13, 2014. The recommended state for this setting is: Disabled. Rationale Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997) Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior for Windows 8.1 and Server 2012 R2.

Failed Instances
i-03e085d4f68678768

18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is: Disabled. Rationale When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Impact: If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

Failed Instances
i-03e085d4f68678768

18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to allow or deny remote access to the Plug and Play interface. The recommended state for this setting is: Disabled. Rationale Allowing remote access to the Plug and Play interface could give hackers another attack vector to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow remote access to the Plug and Play interface Impact: If you disable or do not configure this policy setting, remote connections to the Plug and Play interface are not allowed.

Failed Instances
i-03e085d4f68678768

18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'

Severity
High

Description
Description The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked). Rationale Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to

FALSE (unchecked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Severity
High

Description
Description The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked). Rationale Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. If you enable this policy setting, users on

this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance. To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:<Domain Name>\<User Name> or<Domain Name>\<Group Name> If you enable this policy setting, you should also enable firewall exceptions to allow Remote Assistance communications. The firewall exceptions required for Offer (Unsolicited) Remote Assistance depend on the version of Windows you are running: Windows Vista and later:Enable the Remote Assistance exception for the domain profile. The exception must contain:Port 135:TCP%WINDIR%\System32\msra.exe%WINDIR%\System32\raserver.exe Windows XP with Service Pack 2 (SP2) and Windows XP Professional x64 Edition with Service Pack 1 (SP1):Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe%WINDIR%\System32\Sessmgr.exe For computers running Windows Server 2003 with Service Pack 1 (SP1)Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exeAllow Remote Desktop Exception The recommended state for this setting is: Disabled. Rationale A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance Impact: Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Failed Instances

i-03e085d4f68678768

18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open. The "Select the method for sending email invitations" setting specifies which email standard to use to send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your email message). This policy setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy setting you should also enable appropriate firewall exceptions to allow Remote Assistance communications. The recommended state for this setting is: Disabled. Rationale There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance Impact: If you enable this policy, users on this computer can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and

you can configure additional Remote Assistance settings.If you disable this policy, users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

Failed Instances
i-03e085d4f68678768

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Severity
High

Description
Description This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices Impact: If you enable this policy setting, AutoPlay is not allowed for MTP devices like cameras or phones.

Failed Instances
i-03e085d4f68678768

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Severity
High

Description
Description This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the

installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands. Rationale Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands: Computer Configuration\Policies \Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun Impact: If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to:a) Completely disable autorun commands, orb) Revert back to pre-Windows Vista behavior of automatically executing the autorun command.

Failed Instances
i-03e085d4f68678768

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Severity
High

Description
Description Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: All drives: Computer Configuration\Policies\Administrative Templates \Windows Components\AutoPlay Policies\Turn off Autoplay Impact: Users will have to manually launch setup or installation programs that are provided on removable media.

Failed Instances
i-03e085d4f68678768

18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this setting is: Enabled. Rationale This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button Impact: If you enable this policy setting the password reveal button will not be displayed after a user types a password in the password entry text box. If you disable or do not configure this policy setting the password reveal button will be displayed after a user types a password in the password entry text box. The policy applies to all Windows components and applications that use the Windows system controls including Internet Explorer.

Failed Instances
i-03e085d4f68678768

18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Severity
High

Description
Description By default, all administrator accounts are displayed when you attempt to elevate a running application. The recommended state for this setting is: Disabled. Rationale Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation Impact: If you enable this policy setting, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password. If you disable this policy setting, users will be required to always type in a username and password to elevate.

Failed Instances
i-03e085d4f68678768

18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets. Gadgets are small applets that display information or utilities on the desktop. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn off desktop gadgets Impact: If you enable this setting, desktop gadgets will be turned off.

Failed Instances
i-03e085d4f68678768

18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets that have been installed by the user. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn Off user-installed desktop gadgets Impact: If you enable this setting, Windows will not run any user-installed gadgets.

Failed Instances
i-03e085d4f68678768

18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed

Severity
High

Description
Description The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Rationale EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows

Recommendation
Install EMET 5.5 or higher.

Failed Instances
i-03e085d4f68678768

18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)

Severity

High

Description
Description This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation Settings - EnabledDeep Hooks - EnabledAnti Detours - EnabledBanned Functions - EnabledExploit Action - User Configured Rationale These advanced mitigations for ROP mitigations apply to all configured software in EMET. Deep Hooks protects critical APIs and the subsequent lower level APIs used by the top level critical API. Anti Detours renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue. Banned Functions will block calls to ntdll!LdrHotPatchRoutine to mitigate potential exploits abusing the API.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to Internet Explorer. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\EMET\Default Protections for Internet Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to other popular software. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java. The recommended state for this setting is: Enabled.

Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'

Severity
High

Description
Description This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In. Rationale ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-In: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System ASLR Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'

Severity

High

Description
Description This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System DEP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System SEHOP Note: This Group Policy path

does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to

20 megabytes. The recommended state for this setting is: Enabled: 196,608 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy

setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrativ e Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will

overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you

disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent

to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Severity
High

Description
Description Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled. Rationale Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer Impact: Enabling this policy setting may allow certain legacy plug-in applications to function. Disabling this policy setting will ensure that Data Execution Prevention blocks certain types of malware from exploiting Explorer.

Failed Instances
i-03e085d4f68678768

18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Severity
High

Description
Description Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled. Rationale Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off heap termination on corruption Impact: Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately although Explorer may still terminate unexpectedly later.

Failed Instances
i-03e085d4f68678768

18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled. Rationale Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off shell protocol protected mode Impact: If you enable this policy setting the protocol is fully enabled allowing the opening of folders and files. If you disable this policy setting the protocol is in the protected mode allowing applications to only open a limited set of folders.

Failed Instances
i-03e085d4f68678768

18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Severity
High

Description
Description This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server. The recommended state for this setting is: Enabled. Rationale An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Connection Client \Do not allow passwords to be saved Impact: If you enable this policy setting, the password saving checkbox is disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient \<driveletter>$ If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled. Rationale Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection Impact: Drive redirection will not be possible. In most cases, traditional network drive mapping to file shares (including administrative shares) will serve as a capable substitute to still allow file transfers when needed.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client. Note: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent. The recommended state for this setting is: Enabled. Rationale Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always

prompt for password upon connection Impact: Users will always have to enter their password when they establish new Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled. Rationale Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication Impact: If you enable this policy setting, the terminal server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Severity
High

Description
Description This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and

the client computer for the remote session. The recommended state for this setting is Enabled: High Level. Rationale If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: High Level: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Security\Set client connection encryption level Impact: Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled. Rationale Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Do not delete temp folders upon exit Impact: If you disable this policy setting, temporary folders are deleted when a user logs off, even if the server administrator specifies otherwise.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Severity
High

Description
Description By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled. Rationale By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session Impact: If this setting is enabled, only one temporary folder is used for all remote sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Failed Instances
i-03e085d4f68678768

18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled. Rationale Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures Impact: If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an

enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.

Failed Instances
i-03e085d4f68678768

18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled. Rationale Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: The search service components (including non-Microsoft components) will not encrypted items or encrypted stores.

Failed Instances
i-03e085d4f68678768

18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'

Severity
High

Description
Description This setting allows you to set the default consent handling for error reports. The recommended state for this setting is: Enabled: Always ask before sending data Rationale Error reports may contain sensitive information and should not be sent to anyone automatically.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Always ask before sending data: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\Configure Default consent Impact: By setting to always ask before sending data: Windows prompts users for consent to send reports.

Failed Instances
i-03e085d4f68678768

18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Severity
High

Description
Description Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled. Rationale In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk

unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs Impact: If you disable or do not configure this policy setting, the security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.

Failed Instances
i-03e085d4f68678768

18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Severity
High

Description
Description Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled. Rationale Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

Failed Instances
i-03e085d4f68678768

18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for this setting is: Disabled. Rationale Due to the potential risks of capturing passwords in the logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, logging of PowerShell script input is disabled.

Failed Instances
i-03e085d4f68678768

18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Severity
High

Description
Description This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled. Rationale If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Transcription Note: This Group Policy path does not exist by default. A newer version of the "powershelle xecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the Start-Transcript cmdlet.

Failed Instances
i-03e085d4f68678768

18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication. The

recommended state for this setting is: Enabled. Rationale Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication Impact: The WinRM client will not use Digest authentication.

Failed Instances
i-03e085d4f68678768

18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins

and the RunAsPassword value will be stored securely. If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset. The recommended state for this setting is: Enabled. Rationale Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer.If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Failed Instances
i-03e085d4f68678768

18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If

you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: Enabled. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: 0 - Every day. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped.

The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 0 - Every day: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. The recommended state for this setting is: Disabled. Rationale Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Administrative Templates\Windows Components \Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is displayed in the Shut Down Windows dialog box. The recommended state for this setting is: Disabled. Rationale Alerting users that a system needs to be patch is a good way to help ensure patching is being applied to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be available in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will

notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are:- Enabled- Disabled- Not Configured Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: Disabled. Rationale Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations Impact: If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

Failed Instances
i-03e085d4f68678768

18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. The recommended state for this setting is: Enabled: 1 minute. Rationale Rescheduling automatic updates that were not installed on schedule will help ensure security patches get installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Administrative Templates\Windows

Components\Windows Update\Reschedule Automatic Updates scheduled installations Impact: Remaining Automatic Updates will start 1 minute after the computer restarts.

Failed Instances
i-03e085d4f68678768

4.1.2 Level 1 - Member Server

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Severity
High

Description
Description This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s). Rationale The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their

passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Failed Instances
i-03e085d4f68678768

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'

Severity
High

Description
Description This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s). Rationale Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings \Account Policies\Password Policy\Minimum password age Impact: If an administrator sets a password for a user but wants that user to change the password when the user

first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Failed Instances
i-03e085d4f68678768

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Severity
High

Description
Description This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Rationale Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.Note: Older versions of Windows such

as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Failed Instances
i-03e085d4f68678768

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Severity
High

Description
Description This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0. Rationale Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Failed Instances
i-03e085d4f68678768

2.2.2 (L1) Configure 'Access this computer from the network'

Severity
High

Description
Description This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators, Authenticated Users. Rationale Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Access this computer from the network Impact: If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore it is recommended that it is assigned to the Users group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Failed Instances

i-03e085d4f68678768

2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE: Computer Configuration \Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment \Adjust memory quotas for a process Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Failed Instances
i-03e085d4f68678768

2.2.6 (L1) Configure 'Allow log on locally'

Severity

High

Description
Description This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT +DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators. Rationale Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on locally Impact: If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

Failed Instances
i-03e085d4f68678768

2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'

Severity
High

Description
Description This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application

(such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators. Rationale Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Back up files and directories Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Failed Instances
i-03e085d4f68678768

2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'

Severity
High

Description
Description This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests. Rationale Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a batch job Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Failed Instances
i-03e085d4f68678768

2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'

Severity
High

Description
Description This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests. Note: This security setting does not apply to the System, Local Service, or Network Service accounts. Rationale Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a service Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Failed Instances
i-03e085d4f68678768

2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'

Severity
High

Description
Description This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests. Rationale Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on locally Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Severity
High

Description
Description This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment,

there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account. Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server. Rationale Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests, Local account: Computer Configuration\Policies\Windows Settings \Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Failed Instances
i-03e085d4f68678768

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows

2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

Recommendation
To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Failed Instances
i-03e085d4f68678768

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. Rationale An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Failed Instances
i-03e085d4f68678768

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators. Rationale The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords#x2014;the Primary Domain Controller (PDC) Emulator role.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Shut down the system Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled. Rationale In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is

disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Failed Instances
i-03e085d4f68678768

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'

Severity
High

Description
Description The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). Rationale The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename administrator account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Failed Instances
i-03e085d4f68678768

2.3.1.5 (L1) Configure 'Accounts: Rename guest account'

Severity
High

Description
Description The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. Rationale The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

Failed Instances
i-03e085d4f68678768

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled. Rationale Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Failed Instances
i-03e085d4f68678768

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators. Rationale Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default value. Only Administrators will be able to format and eject removable NTFS media.

Failed Instances
i-03e085d4f68678768

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled. Rationale An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

Failed Instances
i-03e085d4f68678768

2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'

Severity
High

Description

Description This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons#x2014;for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Recommendation

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message text for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances

i-03e085d4f68678768

2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'

Severity

High

Description
Description This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Recommendation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message title for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances
i-03e085d4f68678768

2.3.7.7 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)

Severity
High

Description

Description Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. The recommended state for this setting is: Enabled. Rationale By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account#x2014;such as user rights assignments, account lockout, or the account being disabled#x2014;are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

Recommendation
To implement the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation Impact: When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.

Failed Instances
i-03e085d4f68678768

2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Severity
High

Description

Description This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark. Rationale Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior Impact: If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Failed Instances

i-03e085d4f68678768

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Severity

High

Description

Description This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server

agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session

hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents

session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic

and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances

i-03e085d4f68678768

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Severity
High

Description
Description This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms with the benchmark. Rationale The identity of a computer can be spoofed to gain unauthorized access to network resources.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms with the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Microsoft network server: Server SPN target name validation level Impact: All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Failed Instances
i-03e085d4f68678768

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

Severity
High

Description

Description This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: Disabled. Rationale If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003-based domains. For example, the following computers may not work:Windows NT 4.0-based Remote Access Service servers.Microsoft SQL Servers#x2122; that run on Windows NT 3.x-based or Windows NT 4.0-based computers.Remote Access Service or Microsoft SQL servers that run on Windows 2000-based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Failed Instances
i-03e085d4f68678768

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting

is: Enabled. Rationale An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares Impact: It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Failed Instances
i-03e085d4f68678768

2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Severity
High

Description
Description This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None). Rationale It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously Impact: There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

Failed Instances
i-03e085d4f68678768

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Severity
High

Description
Description When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled. Rationale When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM Impact: If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Failed Instances
i-03e085d4f68678768

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Severity
High

Description
Description Allow NTLM to fall back to NULL session when used with LocalSystem. The default is TRUE up to Windows Vista / Server 2008 and FALSE from Windows 7 / Server 2008 R2 and beyond. The recommended state for this setting is: Disabled. Rationale NULL sessions are less secure because by definition they are unauthenticated.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Failed Instances
i-03e085d4f68678768

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

Severity
High

Description
Description This setting determines if online identities are able to authenticate to this computer. Windows 7 and Windows Server 2008 R2 introduced an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and

associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled. Rationale The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities Impact: Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7 and later.

Failed Instances
i-03e085d4f68678768

2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Severity
High

Description
Description This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types. Rationale The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos Impact: If not selected, the encryption type will not be allowed. This

setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Failed Instances
i-03e085d4f68678768

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

Severity
High

Description
Description LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: Join a domainAuthenticate between Active Directory forestsAuthenticate to down-level domainsAuthenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: Send LM & NTLM responsesSend LM & NTLM #x2014; use NTLMv2 session security if negotiatedSend NTLM responses onlySend NTLMv2 responses onlySend NTLMv2 responses only\refuse LMSend NTLMv2 responses only\refuse LM & NTLMNot Defined The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send LM & NTLM - use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send

NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).These settings correspond to the levels discussed in other Microsoft documents as follows:Level 0 - Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 1 - Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 3 - Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2.Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM. Rationale
In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses#x2014;the weakest form of authentication response#x2014;are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the

Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level Impact: Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Failed Instances
i-03e085d4f68678768

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:- Require message confidentiality. This option is only available in Windows XP and Windows

Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Impact: Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances

i-03e085d4f68678768

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity

High

Description

Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Recommendation

To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Impact: Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use

NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'

Severity
High

Description
Description This security setting determines which subsystems can optionally be started up to support your applications. The recommended state for this setting is: Defined: (blank) Rationale Leaving POSIX enabled could introduce an additional attack surface in your environment.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Defined: (blank) : Computer Configuration\Security Settings\Local Policies\Security Options\System settings: Optional subsystems Impact: Removes POSIX compatibility.

Failed Instances
i-03e085d4f68678768

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: Enabled. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or

administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account Impact: Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Failed Instances
i-03e085d4f68678768

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for administrators. The options are:- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.- Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.- Prompt for consent on the secure desktop: When an

operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: Prompt for consent on the secure desktop. Rationale One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Impact: This policy setting controls the behavior of the elevation prompt for administrators.

Failed Instances
i-03e085d4f68678768

2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for standard users. The options are: Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name

and password. If the user enters valid credentials, the operation continues with the applicable privilege.Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: Automatically deny elevation requests. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users Impact: Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Failed Instances
i-03e085d4f68678768

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off,

Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista / Server 2008 and above, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's

recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\domainfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log. Rationale If events are

not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\domainfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Severity

High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large

number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\privatefw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\privatefw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Private Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale
Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: Yes. Rationale Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No. Rationale When in the Public profile,

there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No. Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\publicfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Public Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security

Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description

Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon.4775: An account could not be mapped for logon.4776: The domain controller attempted to validate the credentials for an account.4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted.Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Application Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis

after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created.4742: A computer account was changed.4743: A computer account was deleted. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Computer Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed.4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Other Account Management Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation

of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created.4728: A member was added to a security-enabled global group.4729: A member was removed from a security-enabled global group.4730: A security-enabled global group was deleted.4731: A security-enabled local group was created.4732: A member was added to a security-enabled local group.4733: A member was removed from a security-enabled local group.4734: A security-enabled local group was deleted.4735: A security-enabled local group was changed.4737: A security-enabled global group was changed.4754: A security-enabled universal group was created.4755: A security-enabled universal group was changed.4756: A member was added to a security-enabled universal group.4757: A member was removed from a security-enabled universal group.4758: A security-enabled universal group was deleted.4764: A group's type was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Security Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed,

disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created.4722: A user account was enabled.4723: An attempt was made to change an account's password.4724: An attempt was made to reset an account's password.4725: A user account was disabled.4726: A user account was deleted.4738: A user account was changed.4740: A user account was locked out.4765: SID History was added to an account.4766: An attempt to add SID History to an account failed.4767: A user account was unlocked.4780: The ACL was set on accounts which are members of administrators groups.4781: The name of an account was changed:4794: An attempt was made to set the Directory Services Restore Mode.5376: Credential Manager credentials were backed up.5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit User Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'

Severity
High

Description
Description This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new

process has been created.4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings \Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected.4778: A session was reconnected to a Window Station.4779: A session was disconnected from a Window Station.4800: The workstation was locked.4801: The workstation was unlocked.4802: The screen saver was invoked.4803: The screen saver was dismissed.5378: The requested credentials delegation was disallowed by policy.5632: A request was made to authenticate to a wireless network.5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed.4719: System audit policy was changed.4902: The Per-user audit policy table was created.4904: An attempt was made to register a security event source.4905: An attempt was made to unregister a security event source.4906: The CrashOnAuditFail value has changed.4907: Auditing settings on object were changed.4908: Special Groups Logon table modified.4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security

incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be

seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.5478: IPsec Services has started successfully.5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown

of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority.4611: A trusted logon process has been registered with the Local Security Authority.4614: A notification package has been loaded by the Security Account Manager.4622: A security package has been loaded by the Local Security Authority.4697: A service was installed in the system. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then

they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file AdmPwd.dll must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you): C:\Program Files\LAPS\CSE\AdmPwd.dll Impact: No impact. When installed and registered properly, AdmPwd.dll takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service.In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Failed Instances
i-03e085d4f68678768

18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to

disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: When you enable this setting, planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Failed Instances
i-03e085d4f68678768

18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage

unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: If you enable this setting, local administrator password is managed. If you disable or not configure this setting, local administrator password is NOT managed.In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Failed Instances
i-03e085d4f68678768

18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS

documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexity option to Large letters + small letters + numbers + special characters : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires password to contain large letters + small letters + numbers + special characters

Failed Instances
i-03e085d4f68678768

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a

Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 15 or more. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Length option to 15 or more : Computer Conf iguration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires the password to have a length of a minimum of 15 characters .

Failed Instances
i-03e085d4f68678768

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small

Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 30 or fewer. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Age (Days) option to 30 or fewer : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires a maximum password age of 30 days or less.

Failed Instances
i-03e085d4f68678768

18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Severity
High

Description
Description This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic

logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled. Rationale If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None. By default this entry is not enabled.

Failed Instances
i-03e085d4f68678768

18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configur ation\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Severity
High

Description
Description Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled. Rationale This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Failed Instances
i-03e085d4f68678768

18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Severity
High

Description
Description NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled. Rationale The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Failed Instances
i-03e085d4f68678768

18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Severity
High

Description
Description The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the

system path first, and then search the current working folder.Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: Enabled. Rationale If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Failed Instances
i-03e085d4f68678768

18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Severity
High

Description
Description Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds. Rationale The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who

could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Failed Instances
i-03e085d4f68678768

18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Severity
High

Description
Description This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less. Rationale If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less: Computer Configuration\Policies\Administrative Templates \MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required -

it is included with Microsoft Security Compliance Manager (SCM). Impact: This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

Failed Instances
i-03e085d4f68678768

18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Severity
High

Description
Description You can use this procedure to enable or disable the user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled. Rationale Allowing users to create a network bridge increases the risk and attack surface from the bridged network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network Impact: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, you can disable the Network Bridge setting on a computer. If you disable Network Bridge on a computer, users cannot create or configure a network bridge. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

Failed Instances
i-03e085d4f68678768

18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled. Rationale Allowing regular users to set a network location increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Require domain users to elevate when setting a network's location Impact: If you enable this policy setting domain users must elevate when setting a network's location. If you disable or do not configure this policy setting domain users can set a network's location without elevating.

Failed Instances
i-03e085d4f68678768

18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Severity
High

Description
Description This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares. Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing. Rationale In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was

not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Failed Instances
i-03e085d4f68678768

18.6.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)

Severity
High

Description
Description This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk. Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the

LocalAccountTokenFilterPolicy registry value to 0. This is the default behavior for Windows. Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about LocalAccountTokenFilterPolicy, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista. The recommended state for this setting is: Enabled. Rationale Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\Apply UAC restrictions to local accounts on network logons Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Severity
High

Description
Description When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is:

Disabled. Rationale Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997) Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior for Windows 8.1 and Server 2012 R2.

Failed Instances
i-03e085d4f68678768

18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is: Disabled. Rationale When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Impact: If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

Failed Instances
i-03e085d4f68678768

18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to allow or deny remote access to the Plug and Play interface. The recommended state for this setting is: Disabled. Rationale Allowing remote access to the Plug and Play interface could give hackers another attack vector to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow remote access to the Plug and Play interface Impact: If you disable or do not configure this policy setting, remote connections to the Plug and Play interface are not allowed.

Failed Instances
i-03e085d4f68678768

18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'

Severity
High

Description
Description The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked). Rationale Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to

FALSE (unchecked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Severity
High

Description
Description The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked). Rationale Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.24.1 (L1) Ensure 'Always use classic logon' is set to 'Enabled'

Severity
High

Description
Description This policy setting forces the user to log on to the computer using the classic logon screen. By default, a workgroup is set to use the simple logon screen. This

setting only works when the computer is not on a domain. The recommended state for this setting is: Enabled. Rationale Explicitly requiring a user to enter their username and password is ideal and a requirement when utilizing the classic logon method. This setting is primarily important because it does not permit the use of a simple logon screen with user accounts presented. (Note: Systems joined to a domain typically are not impacted by this recommendation as username, password, and domain are required for system access. However, this setting is important for standalone systems.)

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Administrative Templates\System\Logon\Always use classic logon Impact: If you enable this policy setting, the classic logon screen is presented to the user at logon, rather than the simple logon screen.

Failed Instances
i-03e085d4f68678768

18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. If you enable this policy setting, users on this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance. To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:<Domain Name>\<User Name> or<Domain Name>\<Group Name> If you enable this policy setting, you should also enable firewall exceptions to allow Remote

Assistance communications. The firewall exceptions required for Offer (Unsolicited) Remote Assistance depend on the version of Windows you are running: Windows Vista and later:Enable the Remote Assistance exception for the domain profile. The exception must contain:Port 135:TCP%WINDIR%\System32\msra.exe%WINDIR%\System32\raserver.exe Windows XP with Service Pack 2 (SP2) and Windows XP Professional x64 Edition with Service Pack 1 (SP1):Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe%WINDIR%\System32\Sessmgr.exe For computers running Windows Server 2003 with Service Pack 1 (SP1)Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exeAllow Remote Desktop Exception The recommended state for this setting is: Disabled. Rationale A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance Impact: Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Failed Instances
i-03e085d4f68678768

18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have

two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open. The "Select the method for sending email invitations" setting specifies which email standard to use to send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your email message). This policy setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy setting you should also enable appropriate firewall exceptions to allow Remote Assistance communications. The recommended state for this setting is: Disabled. Rationale There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance Impact: If you enable this policy, users on this computer can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings.If you disable this policy, users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

Failed Instances

i-03e085d4f68678768

18.8.31.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)

Severity

High

Description

Description This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the trusting domain DCs (see Microsoft KB3073942), so we do not recommend applying it to domain controllers. If you disable this policy setting, RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Endpoint Mapper Service on Windows NT4 Server. If you enable this policy setting, RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service. If you do not configure this policy setting, it remains disabled. RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service. Note: This policy will not be applied until the system is rebooted. The recommended state for this setting is: Enabled. Rationale Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System \Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication Impact: RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Failed Instances

i-03e085d4f68678768

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Severity

High

Description

Description This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices Impact: If you enable this policy setting, AutoPlay is not allowed for MTP devices like cameras or phones.

Failed Instances
i-03e085d4f68678768

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Severity
High

Description
Description This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands. Rationale Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun Impact: If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to:a) Completely disable

autorun commands, orb) Revert back to pre-Windows Vista behavior of automatically executing the autorun command.

Failed Instances
i-03e085d4f68678768

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Severity
High

Description
Description Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: All drives: Computer Configuration\Policies\Administrative Templates \Windows Components\AutoPlay Policies\Turn off Autoplay Impact: Users will have to manually launch setup or installation programs that are provided on removable media.

Failed Instances
i-03e085d4f68678768

18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this

setting is: Enabled. Rationale This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button Impact: If you enable this policy setting the password reveal button will not be displayed after a user types a password in the password entry text box. If you disable or do not configure this policy setting the password reveal button will be displayed after a user types a password in the password entry text box. The policy applies to all Windows components and applications that use the Windows system controls including Internet Explorer.

Failed Instances
i-03e085d4f68678768

18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Severity
High

Description
Description By default, all administrator accounts are displayed when you attempt to elevate a running application. The recommended state for this setting is: Disabled. Rationale Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation Impact: If you enable this policy setting, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password. If you disable this policy setting, users will be required to always type in a username and password to elevate.

Failed Instances
i-03e085d4f68678768

18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets. Gadgets are small applets that display information or utilities on the desktop. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn off desktop gadgets Impact: If you enable this setting, desktop gadgets will be turned off.

Failed Instances
i-03e085d4f68678768

18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets that have been installed by the user. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn Off user-installed desktop gadgets Impact: If you enable this setting, Windows will not run any user-installed gadgets.

Failed Instances

i-03e085d4f68678768

18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed

Severity
High

Description
Description The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Rationale EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows

Recommendation
Install EMET 5.5 or higher.

Failed Instances
i-03e085d4f68678768

18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)

Severity
High

Description
Description This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation Settings - EnabledDeep Hooks - EnabledAnti Detours - EnabledBanned Functions - EnabledExploit Action - User Configured Rationale These advanced mitigations for ROP mitigations apply to all configured software in EMET. Deep Hooks protects critical APIs and the subsequent lower level APIs used by the top level critical API. Anti Detours renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue. Banned Functions will block calls to ntdll!LdrHotPatchRoutine to mitigate potential exploits abusing the API.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\EMET\Default Action and Mitigation Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to Internet Explorer. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Internet Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to other popular software. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'

Severity
High

Description
Description This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In. Rationale ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-In: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System ASLR Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System DEP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System SEHOP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or

may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording

information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log

file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 196,608 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who

successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrativ e Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to

20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Severity
High

Description
Description Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled. Rationale Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Recommendation

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer Impact: Enabling this policy setting may allow certain legacy plug-in applications to function. Disabling this policy setting will ensure that Data Execution Prevention blocks certain types of malware from exploiting Explorer.

Failed Instances
i-03e085d4f68678768

18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Severity
High

Description
Description Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled. Rationale Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off heap termination on corruption Impact: Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately although Explorer may still terminate unexpectedly later.

Failed Instances
i-03e085d4f68678768

18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol

applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled. Rationale Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off shell protocol protected mode Impact: If you enable this policy setting the protocol is fully enabled allowing the opening of folders and files. If you disable this policy setting the protocol is in the protected mode allowing applications to only open a limited set of folders.

Failed Instances
i-03e085d4f68678768

18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Severity
High

Description
Description This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server. The recommended state for this setting is: Enabled. Rationale An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Connection Client \Do not allow passwords to be saved Impact: If you enable this policy setting, the

password saving checkbox is disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient \<driveletter>$ If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled. Rationale Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection Impact: Drive redirection will not be possible. In most cases, traditional network drive mapping to file shares (including administrative shares) will serve as a capable substitute to still allow file transfers when needed.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Severity
High

Description

Description This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client. Note: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent. The recommended state for this setting is: Enabled. Rationale Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection Impact: Users will always have to enter their password when they establish new Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled. Rationale Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication Impact: If you enable this policy setting, the terminal server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Severity
High

Description
Description This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. The recommended state for this setting is Enabled: High Level. Rationale If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: High Level: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Security\Set client connection encryption level Impact: Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled. Rationale Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Do not delete temp folders upon exit Impact: If you disable this policy setting, temporary folders are deleted when a user logs off, even if the server administrator specifies otherwise.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Severity
High

Description
Description By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled. Rationale By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session Impact: If this setting is enabled, only

one temporary folder is used for all remote sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Failed Instances
i-03e085d4f68678768

18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled. Rationale Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures Impact: If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.

Failed Instances
i-03e085d4f68678768

18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will

be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled. Rationale Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: The search service components (including non-Microsoft components) will not encrypted items or encrypted stores.

Failed Instances
i-03e085d4f68678768

18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'

Severity
High

Description
Description This setting allows you to set the default consent handling for error reports. The recommended state for this setting is: Enabled: Always ask before sending data Rationale Error reports may contain sensitive information and should not be sent to anyone automatically.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Always ask before sending data: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\Configure Default consent Impact: By setting to always ask before sending data: Windows prompts users for consent to send reports.

Failed Instances
i-03e085d4f68678768

18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Severity
High

Description
Description Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled. Rationale In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs Impact: If you disable or do not configure this policy setting, the security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.

Failed Instances
i-03e085d4f68678768

18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Severity
High

Description

Description Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled. Rationale Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

Failed Instances
i-03e085d4f68678768

18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for

this setting is: Disabled. Rationale Due to the potential risks of capturing passwords in the logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, logging of PowerShell script input is disabled.

Failed Instances
i-03e085d4f68678768

18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Severity
High

Description
Description This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled. Rationale If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Transcription Note: This Group Policy path does not exist by default. A newer version of the "powershelle xecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the Start-Transcript cmdlet.

Failed Instances
i-03e085d4f68678768

18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM

network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication. The recommended state for this setting is: Enabled. Rationale Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication Impact: The WinRM client will not use Digest authentication.

Failed Instances
i-03e085d4f68678768

18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely. If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset. The recommended state for this setting is: Enabled. Rationale Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on

this computer.If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Failed Instances
i-03e085d4f68678768

18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: Enabled. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: 0 - Every day. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 0 - Every day: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'

Severity

High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. The recommended state for this setting is: Disabled. Rationale Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Administrative Templates\Windows Components \Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is displayed in the Shut Down Windows dialog box. The recommended state for this setting is: Disabled. Rationale Alerting users that a system needs to be patch is a good way to help ensure patching is being applied to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be available in the Shut Down

Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are:- Enabled- Disabled- Not Configured Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: Disabled. Rationale Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations Impact: If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

Failed Instances
i-03e085d4f68678768

18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. The recommended state for this setting is: Enabled: 1 minute. Rationale Rescheduling automatic updates that were not installed on schedule will help ensure security patches get installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations Impact: Remaining Automatic Updates will start 1 minute after the computer restarts.

Failed Instances
i-03e085d4f68678768

4.1.3 Level 2 - Domain Controller

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Severity
High

Description
Description This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended

state for this setting is: 24 or more password(s). Rationale The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Failed Instances
i-03e085d4f68678768

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'

Severity
High

Description
Description This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s). Rationale Users may have favorite passwords that they like

to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings \Account Policies\Password Policy\Minimum password age Impact: If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Failed Instances
i-03e085d4f68678768

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Severity
High

Description
Description This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet

your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Rationale Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Failed Instances
i-03e085d4f68678768

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Severity
High

Description
Description This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0. Rationale Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Failed Instances
i-03e085d4f68678768

2.2.2 (L1) Configure 'Access this computer from the network'

Severity
High

Description
Description This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators, Authenticated Users. Rationale Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the

default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Access this computer from the network Impact: If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore it is recommended that it is assigned to the Users group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Failed Instances
i-03e085d4f68678768

2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE: Computer Configuration \Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment \Adjust memory quotas for a process Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Failed Instances
i-03e085d4f68678768

2.2.6 (L1) Configure 'Allow log on locally'

Severity
High

Description
Description This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT +DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators. Rationale Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on locally Impact: If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

Failed Instances
i-03e085d4f68678768

2.2.7 (L1) Configure 'Allow log on through Remote Desktop Services'

Severity
High

Description
Description This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the restricted groups feature to ensure that no user accounts are part of the Remote Desktop Users group. Restrict this user right to the Administrators group, and possibly the Remote Desktop Users group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: Administrators, Remote Desktop Users. Note: A server that holds the Remote Desktop Services Role with Remote Desktop Connection Broker Role Service will require a special exception to this recommendation, to allow the Authenticated Users group to be granted this user right. Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass. Rationale Any account with the Allow log on through Terminal Services user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on through Remote Desktop Services Impact: Removal of the Allow log on through Terminal Services user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'

Severity
High

Description
Description This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators. Rationale Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Back up files and directories Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Failed Instances
i-03e085d4f68678768

2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'

Severity
High

Description
Description This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests. Rationale Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a batch job Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Failed Instances
i-03e085d4f68678768

2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'

Severity
High

Description

Description This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests. Note: This security setting does not apply to the System, Local Service, or Network Service accounts. Rationale Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a service Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Failed Instances

i-03e085d4f68678768

2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'

Severity

High

Description

Description This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests. Rationale Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on locally Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Severity
High

Description
Description This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account. Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server. Rationale Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests, Local account: Computer Configuration\Policies\Windows Settings \Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Failed Instances
i-03e085d4f68678768

2.2.25 (L1) Configure 'Impersonate a client after authentication'

Severity
High

Description
Description The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect#x2014;for example, by remote procedure call (RPC) or named pipes#x2014;to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels. Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started. Also, a user can impersonate an access token if any of the following conditions exist:- The access token that is being impersonated is for this user.- The user, in this logon session, logged on to the network with explicit credentials to create the access token.- The requested level is less than Impersonate, such as Anonymous or Identify. An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE .Level 1 - Member Server. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS. Rationale An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies

\User Rights Assignment\Impersonate a client after authentication Impact: In most cases this configuration will have no impact. If you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to also assign the user right to IIS_IUSRS.

Failed Instances
i-03e085d4f68678768

2.2.29 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only)

Severity
High

Description
Description This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in enterprise environments. However, its use should be restricted in high security environments to prevent misuse of system resources or to prevent attackers from using the right to launch malicious code after gaining user level access to a computer. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers. The recommended state for this setting is: Administrators. Rationale The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Administrators: Computer Configuration\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Log on as a batch job Impact: If you configure the Log on as a batch job setting through domain-based Group Policies, the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the Task Scheduler. If you install optional components such as ASP.NET or IIS, you might need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the IIS_WPG group and the IUSR_<ComputerName>, ASPNET, and IWAM_<ComputerName> accounts. If this user right is not assigned to this group and these accounts, IIS will be unable to run some COM objects that are necessary for proper functionality.

Failed Instances

i-03e085d4f68678768

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

Recommendation
To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Failed Instances
i-03e085d4f68678768

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Severity
High

Description

Description This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. Rationale An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Failed Instances

i-03e085d4f68678768

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'

Severity

High

Description

Description This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators. Rationale The ability to

shut down domain controllers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords#x2014;the Primary Domain Controller (PDC) Emulator role.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Shut down the system Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled. Rationale In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a

prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Failed Instances
i-03e085d4f68678768

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'

Severity
High

Description
Description The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). Rationale The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account

has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename administrator account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Failed Instances
i-03e085d4f68678768

2.3.1.5 (L1) Configure 'Accounts: Rename guest account'

Severity
High

Description
Description The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. Rationale The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

Failed Instances
i-03e085d4f68678768

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled. Rationale Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Failed Instances
i-03e085d4f68678768

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators. Rationale Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default value. Only Administrators will be able to format and eject removable NTFS media.

Failed Instances
i-03e085d4f68678768

2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)

Severity
High

Description
Description This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account

with which the user authenticates when they set up the job. Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu. The recommended state for this setting is: Disabled. Rationale If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks Impact: The impact should be small for most organizations. Users (including those in the Server Operators group) will still be able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Failed Instances
i-03e085d4f68678768

2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)

Severity
High

Description
Description This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. The recommended state for this setting is: Require signing. Rationale Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement

Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Require signing: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Domain controller: LDAP server signing requirements Impact: Clients that do not support LDAP signing will be unable to run LDAP queries against the domain controllers. All Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see Microsoft Knowledge Base article 325465: Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools. Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Failed Instances
i-03e085d4f68678768

2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)

Severity
High

Description
Description This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password.Default: This policy is not defined, which means that the system treats it as Disabled. The recommended state for this setting is: Disabled. Rationale If you enable this policy setting on all domain controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes Impact: None. This is the default configuration.

Failed Instances
i-03e085d4f68678768

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled. Rationale An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

Failed Instances
i-03e085d4f68678768

2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'

Severity
High

Description

Description This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons#x2014;for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Recommendation

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message text for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances

i-03e085d4f68678768

2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'

Severity

High

Description

Description This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Recommendation

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message title for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances

i-03e085d4f68678768

2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Severity

High

Description

Description This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark. Rationale Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior Impact: If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Failed Instances
i-03e085d4f68678768

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set

this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers

running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-

middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively,

the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Severity

High

Description

Description This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms with the benchmark. Rationale The identity of a computer can be spoofed to gain unauthorized access to network resources.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms with the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Microsoft network server: Server SPN target name validation level Impact: All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Failed Instances

i-03e085d4f68678768

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

Severity

High

Description

Description This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: Disabled. Rationale If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003-based domains. For example, the following computers may not work:Windows NT 4.0-based Remote Access Service servers.Microsoft SQL Servers#x2122; that run on Windows NT 3.x-based or Windows NT 4.0-based computers.Remote Access Service or Microsoft SQL servers that run on Windows 2000-based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Failed Instances
i-03e085d4f68678768

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting

is: Enabled. Rationale An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares Impact: It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Failed Instances
i-03e085d4f68678768

2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the Stored User Names and Passwords feature may save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the Stored User Names and Passwords feature of Windows does not store passwords and credentials. The recommended state for this setting is: Enabled. Rationale Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication Impact: Users will be forced to enter passwords

whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Failed Instances
i-03e085d4f68678768

2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously'

Severity
High

Description
Description This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. The recommended state for this setting is: Level 1 - Domain Controller. The recommended state for this setting is: LSARPC, NETLOGON, SAMR and (when the legacy Computer Browser service is enabled) BROWSER.Level 1 - Member Server. The recommended state for this setting is: <blank> (i.e. None), or (when the legacy Computer Browser service is enabled) BROWSER. Note: A server that holds the Remote Desktop Services Role with Remote Desktop Licensing Role Service will require a special exception to this recommendation, to allow the HydraLSPipe and TermServLicensing Named Pipes to be accessed anonymously. Rationale Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Network access: Named Pipes that can be accessed anonymously Impact: This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The BROWSER named pipe may need to be added to this list if the

Computer Browser service is needed for supporting legacy components. The Computer Browser service is disabled by default.

Failed Instances
i-03e085d4f68678768

2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Severity
High

Description
Description This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None). Rationale It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously Impact: There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

Failed Instances
i-03e085d4f68678768

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Severity
High

Description
Description When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the

negotiation. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled. Rationale When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM Impact: If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Failed Instances
i-03e085d4f68678768

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Severity
High

Description
Description Allow NTLM to fall back to NULL session when used with LocalSystem. The default is TRUE up to Windows Vista / Server 2008 and FALSE from Windows 7 / Server 2008 R2 and beyond. The recommended state for this setting is: Disabled. Rationale NULL sessions are less secure because by definition they are unauthenticated.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Failed Instances
i-03e085d4f68678768

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

Severity
High

Description
Description This setting determines if online identities are able to authenticate to this computer. Windows 7 and Windows Server 2008 R2 introduced an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled. Rationale The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities Impact: Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7 and later.

Failed Instances
i-03e085d4f68678768

2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Severity
High

Description
Description This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types. Rationale The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos Impact: If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Failed Instances
i-03e085d4f68678768

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

Severity
High

Description

Description LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: Join a domainAuthenticate between Active Directory forestsAuthenticate to down-level domainsAuthenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: Send LM & NTLM responsesSend LM & NTLM #x2014; use NTLMv2 session security if negotiatedSend NTLM responses onlySend NTLMv2 responses onlySend NTLMv2 responses only\refuse LMSend NTLMv2 responses only\refuse LM & NTLMNot Defined The Network security: LAN Manager authentication level setting determines which challenge/ response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send LM & NTLM - use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).These settings correspond to the levels discussed in other Microsoft documents as follows:Level 0 - Send LM and NTLM response; never use

NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 1 - Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 3 - Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2.Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM. Rationale
In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses#x2014;the weakest form of authentication response#x2014;are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Recommendation

To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies

\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level Impact: Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Failed Instances
i-03e085d4f68678768

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for

this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Impact: Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This

option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Impact: Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'

Severity
High

Description
Description This security setting determines which subsystems can optionally be started up to support your applications. The recommended state for this setting is: Defined:

(blank) Rationale Leaving POSIX enabled could introduce an additional attack surface in your environment.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Defined: (blank) : Computer Configuration\Security Settings\Local Policies\Security Options\System settings: Optional subsystems Impact: Removes POSIX compatibility.

Failed Instances
i-03e085d4f68678768

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: Enabled. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account Impact: Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Failed Instances
i-03e085d4f68678768

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for administrators. The options are:- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.- Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.- Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: Prompt

for consent on the secure desktop. Rationale One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Impact: This policy setting controls the behavior of the elevation prompt for administrators.

Failed Instances
i-03e085d4f68678768

2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for standard users. The options are: Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: Automatically deny elevation requests. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under

elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users Impact: Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Failed Instances
i-03e085d4f68678768

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista / Server 2008 and above, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those

specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact:

If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured

by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\domainfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\domainfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale
Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\privatefw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\privatefw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Private Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit

(KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The

recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before

deploying. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: Yes. Rationale Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows

Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No. Rationale When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Severity
High

Description

Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No. Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\publicfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Public Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it

may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon.4775: An account could not be mapped for logon.4776: The domain controller attempted to validate the credentials for an account.4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted.Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Application Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created.4742: A computer account was changed.4743: A computer account was deleted.

The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Computer Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include: 4744: A security-disabled local group was created.4745: A security-disabled local group was changed.4746: A member was added to a security-disabled local group.4747: A member was removed from a security-disabled local group.4748: A security-disabled local group was deleted.4749: A security-disabled global group was created.4750: A security-disabled global group was changed.4751: A member was added to a security-disabled global group.4752: A member was removed from a security-disabled global group.4753: A security-disabled global group was deleted.4759: A security-disabled universal group was created.4760: A security-disabled universal group was changed.4761: A member was added to a

security-disabled universal group.4762: A member was removed from a security-disabled universal group.4763: A security-disabled universal group was deleted. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may provide an organization with insight when investigating an incident. For example, when a given unauthorized user was added to a sensitive distribution group.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Distribution Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed.4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management

\Audit Other Account Management Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created.4728: A member was added to a security-enabled global group.4729: A member was removed from a security-enabled global group.4730: A security-enabled global group was deleted.4731: A security-enabled local group was created.4732: A member was added to a security-enabled local group.4733: A member was removed from a security-enabled local group.4734: A security-enabled local group was deleted.4735: A security-enabled local group was changed.4737: A security-enabled global group was changed.4754: A security-enabled universal group was created.4755: A security-enabled universal group was changed.4756: A member was added to a security-enabled universal group.4757: A member was removed from a security-enabled universal group.4758: A security-enabled universal group was deleted.4764: A group's type was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Security Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created.4722: A user account was enabled.4723: An attempt was made to change an account's password.4724: An attempt was made to reset an account's password.4725: A user account was disabled.4726: A user account was deleted.4738: A user account was changed.4740: A user account was locked out.4765: SID History was added to an account.4766: An attempt to add SID History to an account failed.4767: A user account was unlocked.4780: The ACL was set on accounts which are members of administrators groups.4781: The name of an account was changed:4794: An attempt was made to set the Directory Services Restore Mode.5376: Credential Manager credentials were backed up.5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit User Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'

Severity
High

Description
Description This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created.4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings \Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected.

Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.4.1 (L1) Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to domain controllers. Events for this subcategory include: 4662 : An operation was performed on an object. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only)

Severity
High

Description
Description This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers. Events for this subcategory include: 5136 : A directory service object was modified.5137 : A directory service object was created.5138 : A directory service object was undeleted.5139 : A directory service object was moved. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure. Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Changes Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Severity
High

Description

Description This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected.4778: A session was reconnected to a Window Station.4779: A session was disconnected from a Window Station.4800: The workstation was locked.4801: The workstation was unlocked.4802: The screen saver was invoked.4803: The screen saver was dismissed.5378: The requested credentials delegation was disallowed by policy.5632: A request was made to authenticate to a wireless network.5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances

i-03e085d4f68678768

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'

Severity

High

Description

Description This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed.4719: System audit policy was changed.4902: The Per-user audit policy table was created.4904: An attempt was made to register a security event source.4905: An

attempt was made to unregister a security event source.4906: The CrashOnAuditFail value has changed.4907: Auditing settings on object were changed.4908: Special Groups Logon table modified.4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object.

The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning

hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.5478: IPsec Services has started successfully.5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances

i-03e085d4f68678768

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'

Severity

High

Description
Description This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority.4611: A trusted logon process has been registered with the Local Security Authority.4614: A notification package has been loaded by the Security Account Manager.4622: A security package has been loaded by the Local Security Authority.4697: A service was installed in the system. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Severity
High

Description
Description This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any

network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled. Rationale If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None. By default this entry is not enabled.

Failed Instances
i-03e085d4f68678768

18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configur ation\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Severity
High

Description
Description Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled. Rationale This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Failed Instances
i-03e085d4f68678768

18.3.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'

Severity
High

Description
Description This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet. The recommended state for this setting is: Enabled: 300,000 or 5 minutes (recommended). Rationale An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 300,000 or 5 minutes (recommended) : Computer Configuration\Policies \Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Failed Instances
i-03e085d4f68678768

18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Severity
High

Description
Description NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled. Rationale The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would

cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Failed Instances
i-03e085d4f68678768

18.3.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'

Severity
High

Description
Description This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis. The recommended state for this setting is: Disabled. Rationale An attacker who has gained control of a computer on the same network segment could configure a computer on the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default

Gateway addresses (could lead to DoS) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: If you disable this entry, Windows Server 2003 (which supports the IRDP) cannot automatically detect and configure default gateway addresses on the computer.

Failed Instances
i-03e085d4f68678768

18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Severity
High

Description
Description The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the system path first, and then search the current working folder.Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: Enabled. Rationale If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Failed Instances
i-03e085d4f68678768

18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Severity
High

Description
Description Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds. Rationale The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/ adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Failed Instances
i-03e085d4f68678768

18.3.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Severity
High

Description
Description This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3. Rationale A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 3: Computer Configuration\Policies\Administrative Templates\MSS (Legacy) \MSS:(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Failed Instances
i-03e085d4f68678768

18.3.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Severity
High

Description
Description This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3. Rationale A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 3: Computer Configuration\Policies\Administrative Templates\MSS (Leg acy)\MSS:(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Failed Instances
i-03e085d4f68678768

18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Severity
High

Description
Description This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less. Rationale If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less: Computer Configuration\Policies\Administrative Templates \MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: This setting

will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

Failed Instances
i-03e085d4f68678768

18.4.8.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'

Severity
High

Description
Description This policy setting changes the operational behavior of the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Rationale To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver Impact: If you disable or do not configure this policy setting, the default behavior of LLTDIO will apply.

Failed Instances
i-03e085d4f68678768

18.4.8.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'

Severity
High

Description
Description This policy setting changes the operational behavior of the Responder network protocol driver. The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It

also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Rationale To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver Impact: If you disable or do not configure this policy setting, the default behavior of RSPNDR will apply.

Failed Instances
i-03e085d4f68678768

18.4.9.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'

Severity
High

Description
Description The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPV6 address and port number. The protocol operates in the context of clouds . A cloud is a set of peer computers that can communicate with each other by using the same IPv6 scope. Peer-to-Peer protocols allow for applications in the areas of RTC, collaboration, content distribution and distributed processing. The recommended state for this setting is: Enabled. Rationale This setting enhances the security of the environment and reduces the overall risk exposure related to peer-to-peer networking.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Microsoft Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking Services Impact: If you enable this setting, peer-to-peer protocols will be turned off. If you disable this setting or do not configure it, the peer-to-peer protocols

will be turned on. This setting turns off Microsoft Peer-to-Peer Networking Services in its entirety, and will cause all dependent applications to stop working.

Failed Instances
i-03e085d4f68678768

18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Severity
High

Description
Description You can use this procedure to enable or disable the user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled. Rationale Allowing users to create a network bridge increases the risk and attack surface from the bridged network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network Impact: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, you can disable the Network Bridge setting on a computer. If you disable Network Bridge on a computer, users cannot create or configure a network bridge. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

Failed Instances
i-03e085d4f68678768

18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'

Severity

High

Description
Description This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled. Rationale Allowing regular users to set a network location increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Require domain users to elevate when setting a network's location Impact: If you enable this policy setting domain users must elevate when setting a network's location. If you disable or do not configure this policy setting domain users can set a network's location without elevating.

Failed Instances
i-03e085d4f68678768

18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Severity
High

Description
Description This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares. Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing. Rationale In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (NetworkProvider.admx/

adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1* \SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: * \NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Polici es\Administrative Templates\Network\Network Provider\Hardened UNC Paths Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Failed Instances
i-03e085d4f68678768

18.4.18.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')

Severity
High

Description
Description Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6 allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively. The recommended state for this setting is: DisabledComponents - 0xff (255) Rationale Since the vast majority of private corporate networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling IPv6 components reduces a possible attack surface

that is also harder to monitor the traffic on. As a result, we recommend configuring IPv6 to a Disabled state when it is not needed.

Recommendation
To establish the recommended configuration, set the following Registry value to 0xff (255) (DWORD): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TCPIP6\Parameters:DisabledComponents Note: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (Disable -IPv6-Components-KB929852.adm) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state. Impact: Connectivity to other systems using IPv6 will no longer operate, and software that depends on IPv6 will cease to function. Examples of Microsoft applications that may use IPv6 include: Remote Assistance, HomeGroup, DirectAccess, Windows Mail.This registry change is documented in Microsoft Knowledge Base article 929852: How to disable IPv6 or its components in Windows.Note: This registry change does not take effect until the next reboot.

Failed Instances
i-03e085d4f68678768

18.4.19.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over In-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. The recommended state for this setting is: Disabled. Rationale This setting enhances the security of the environment and reduces the overall risk exposure related to user configuration of wireless settings.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Network \Windows Connect Now\Configuration of wireless settings using Windows Connect Now Impact: If you enable this policy setting additional choices are available to turn off the operations over a specific medium. If you disable this policy setting operations are disabled over all media. If you do not configure this policy setting operations are enabled over all media.

Failed Instances
i-03e085d4f68678768

18.4.19.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'

Severity
High

Description
Description This policy setting prohibits access to Windows Connect Now (WCN) wizards. The recommended state for this setting is: Enabled. Rationale Allowing standard users to access the Windows Connect Now wizard increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Network\Network \Windows Connect Now\Prohibit access of the Windows Connect Now wizards Impact: If you enable this policy setting the wizards are turned off and users have no access to any of the wizard tasks. All the configuration related tasks including "Set up a wireless router or access point" and "Add a wireless device" are disabled. If you disable or do not configure this policy setting users can access the wizard tasks including "Set up a wireless router or access point" and "Add a wireless device."

Failed Instances
i-03e085d4f68678768

18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Severity

High

Description
Description When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is: Disabled. Rationale Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997) Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior for Windows 8.1 and Server 2012 R2.

Failed Instances
i-03e085d4f68678768

18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is: Disabled. Rationale When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created

process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Impact: If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

Failed Instances
i-03e085d4f68678768

18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to allow or deny remote access to the Plug and Play interface. The recommended state for this setting is: Disabled. Rationale Allowing remote access to the Plug and Play interface could give hackers another attack vector to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow remote access to the Plug and Play interface Impact: If you disable or do not configure this policy setting, remote connections to the Plug and Play interface are not allowed.

Failed Instances
i-03e085d4f68678768

18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'

Severity
High

Description
Description The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked). Rationale Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Severity
High

Description
Description The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked). Rationale Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies

will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.19.1.1 (L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP. The recommended state for this setting is: Enabled. Rationale Users might download drivers that include malicious code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP Impact: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits drivers that are not already installed locally from downloading.

Failed Instances
i-03e085d4f68678768

18.8.19.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'

Severity
High

Description
Description This setting turns off data sharing from the handwriting recognition personalization tool. The handwriting recognition personalization tool enables Tablet PC users to adapt handwriting recognition to their own writing style by providing

writing samples. The tool can optionally share user writing samples with Microsoft to improve handwriting recognition in future versions of Windows. The tool generates reports and transmits them to Microsoft over a secure connection. The recommended state for this setting is: Enabled. Rationale A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting personalization data sharing Note: This Group Policy setting is provided by the Group Policy template "ShapeCollector.admx/adml" that is included with the Microsoft Windows 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: If you enable this policy, Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

Failed Instances
i-03e085d4f68678768

18.8.19.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'

Severity
High

Description
Description Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. The recommended state for this setting is: Enabled. Rationale A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting recognition error reporting Impact: If you enable this policy, users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

Failed Instances
i-03e085d4f68678768

18.8.19.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs). The recommended state for this setting is: Enabled. Rationale In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com Impact: If you enable this policy setting, the "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

Failed Instances
i-03e085d4f68678768

18.8.19.1.5 (L2) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

Severity
High

Description

Description This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards. The recommended state for this setting is: Enabled. Rationale Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards Impact: If this policy setting is enabled, Windows is prevented from downloading providers; only the service providers cached in the local registry will display.

Failed Instances
i-03e085d4f68678768

18.8.19.1.6 (L2) Ensure 'Turn off Internet File Association service' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to use the Microsoft Web service for finding an application to open a file with an unhandled file association. When a user opens a file that has an extension that is not associated with any applications on the computer, the user is given the choice to select a local application or use the Web service to find an application. The recommended state for this setting is: Enabled. Rationale This service#x2019;s purpose is to help find an appropriate application for a file whose type is unrecognized by the computer. That could pose a security risk if the unrecognized file is malicious code, even if the application to be discovered is itself innocent. Corporate environments tend to be very managed, where the IT staff decide which applications should and should not be installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet File

Association service Impact: If you enable this policy setting, the link and the dialog for using the Web service to open an unhandled file association are removed.

Failed Instances
i-03e085d4f68678768

18.8.19.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet. The recommended state for this setting is: Enabled. Rationale Information that is transmitted over HTTP through this capability is not protected and can be intercepted by malicious users. For this reason, it is not often used in enterprise environments.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP Impact: If you enable this policy setting, the client computer will not be able to print to Internet printers over HTTP. This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

Failed Instances
i-03e085d4f68678768

18.8.19.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration. The recommended state for

this setting is: Enabled. Rationale Users in a corporate environment should not be registering their own copies of Windows, providing their own PII in the process.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registration if URL connection is referring to Microsoft.com Impact: If you enable this policy setting, it blocks users from connecting to Microsoft.com for online registration and users cannot register their copy of Windows online.

Failed Instances
i-03e085d4f68678768

18.8.19.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches. The recommended state for this setting is: Enabled. Rationale There is a small risk that users will unknowingly reveal sensitive information because of the topics they are searching for. This risk is very low because even if this setting is enabled users still must submit search queries to the desired search engine in order to perform searches.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates Impact: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.

Failed Instances

i-03e085d4f68678768

18.8.19.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the "Order Prints Online" task is available from Picture Tasks in Windows folders. The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online. The recommended state for this setting is: Enabled. Rationale In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task Impact: If you enable this policy setting, the task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Failed Instances
i-03e085d4f68678768

18.8.19.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web are available from File and Folder Tasks in Windows folders. The recommended state for this setting is: Enabled. Rationale Users may publish confidential or sensitive information to a public service outside of the control of the organization.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet

Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders Impact: The Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.

Failed Instances
i-03e085d4f68678768

18.8.19.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. The recommended state for this setting is: Enabled. Rationale Large enterprise environments may not want to have information collected from managed client computers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program Impact: Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

Failed Instances
i-03e085d4f68678768

18.8.19.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

Severity
High

Description

Description This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. The recommended state for this setting is: Enabled. Rationale Large enterprise environments may not want to have information collected from managed client computers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program Impact: Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

Failed Instances
i-03e085d4f68678768

18.8.19.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls whether or not errors are reported to Microsoft. Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product. The recommended state for this setting is: Enabled. Rationale If a Windows Error occurs in a secure, managed corporate environment, the error should be reported directly to IT staff for troubleshooting and remediation. There is no benefit to the corporation to report these errors directly to Microsoft, and there is some risk of unknowingly exposing sensitive data as part of the error.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Error Reporting Impact: If you enable this policy setting, users are not given the option to report errors.

Failed Instances
i-03e085d4f68678768

18.8.28.4.1 (L2) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

Severity
High

Description
Description Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled. Rationale Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery) Impact: If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep.If you disable this policy, the user is not prompted for a password when the system resumes from sleep.

Failed Instances
i-03e085d4f68678768

18.8.28.4.2 (L2) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

Severity
High

Description
Description Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled. Rationale Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in) Impact: If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep.If you disable this policy, the user is not prompted for a password when the system resumes from sleep.

Failed Instances
i-03e085d4f68678768

18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. If you enable this policy setting, users on this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance. To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:<Domain Name>\<User Name> or<Domain Name>\<Group Name> If you enable this policy setting, you should also enable firewall exceptions to allow Remote Assistance communications. The firewall exceptions required for Offer (Unsolicited) Remote Assistance depend on the version of Windows you are running: Windows Vista and later:Enable the Remote Assistance exception for the domain profile. The exception must contain:Port 135:TCP%WINDIR%\System32\msra.exe%WINDIR%\System32\raserver.exe Windows XP with Service Pack 2 (SP2) and Windows XP Professional x64

Edition with Service Pack 1 (SP1):Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe%WINDIR%\System32\Sessmgr.exe For computers running Windows Server 2003 with Service Pack 1 (SP1)Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exeAllow Remote Desktop Exception The recommended state for this setting is: Disabled. Rationale A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance Impact: Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Failed Instances
i-03e085d4f68678768

18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open. The "Select the method for sending email invitations" setting specifies which email standard to use to

send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your email message). This policy setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy setting you should also enable appropriate firewall exceptions to allow Remote Assistance communications. The recommended state for this setting is: Disabled. Rationale There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance Impact: If you enable this policy, users on this computer can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings.If you disable this policy, users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

Failed Instances
i-03e085d4f68678768

18.8.38.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'

Severity
High

Description
Description This policy setting configures Microsoft Support Diagnostic Tool (MSDT) interactive communication with the support provider. MSDT gathers diagnostic data for analysis by support professionals. The recommended state for this setting is: Disabled.

Rationale Due to privacy concerns, data should never be sent to any 3rd party since this data could contain sensitive information.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Tro ubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider Impact: If you disable this policy setting, MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Failed Instances
i-03e085d4f68678768

18.8.38.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether to enable or disable tracking of responsiveness events. The recommended state for this setting is: Disabled. Rationale When enabled the aggregated data of a given event will be transmitted to Microsoft. The option exists to restrict this feature for a specific user, set the consent level, and designate specific programs for which error reports could be sent. However, centrally restricting the ability to execute PerfTrack to limit the potential for unauthorized or undesired usage, data leakage, or unintentional communications is highly recommended.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Trouble shooting and Diagnostics\Windows Performance PerfTrack\Enable/Disable PerfTrack Impact: If you disable this policy setting, responsiveness events are not processed.

Failed Instances
i-03e085d4f68678768

18.8.43.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider. The recommended state for this setting is: Enabled. Rationale A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client Impact: If you enable this policy setting, you can set the local computer clock to synchronize time with NTP servers.

Failed Instances
i-03e085d4f68678768

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Severity
High

Description
Description This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices Impact: If

you enable this policy setting, AutoPlay is not allowed for MTP devices like cameras or phones.

Failed Instances
i-03e085d4f68678768

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Severity
High

Description
Description This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands. Rationale Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands: Computer Configuration\Policies \Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun Impact: If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to:a) Completely disable autorun commands, orb) Revert back to pre-Windows Vista behavior of automatically executing the autorun command.

Failed Instances
i-03e085d4f68678768

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Severity
High

Description
Description Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: All drives: Computer Configuration\Policies\Administrative Templates \Windows Components\AutoPlay Policies\Turn off Autoplay Impact: Users will have to manually launch setup or installation programs that are provided on removable media.

Failed Instances
i-03e085d4f68678768

18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this setting is: Enabled. Rationale This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button Impact: If you enable this policy setting the password reveal button will not be displayed after a user types a password in the password entry text box. If you disable or

do not configure this policy setting the password reveal button will be displayed after a user types a password in the password entry text box. The policy applies to all Windows components and applications that use the Windows system controls including Internet Explorer.

Failed Instances
i-03e085d4f68678768

18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Severity
High

Description
Description By default, all administrator accounts are displayed when you attempt to elevate a running application. The recommended state for this setting is: Disabled. Rationale Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation Impact: If you enable this policy setting, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password. If you disable this policy setting, users will be required to always type in a username and password to elevate.

Failed Instances
i-03e085d4f68678768

18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'

Severity
High

Description

Description This policy setting allows you to turn off desktop gadgets. Gadgets are small applets that display information or utilities on the desktop. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn off desktop gadgets Impact: If you enable this setting, desktop gadgets will be turned off.

Failed Instances
i-03e085d4f68678768

18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets that have been installed by the user. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn Off user-installed desktop gadgets Impact: If you enable this setting, Windows will not run any user-installed gadgets.

Failed Instances
i-03e085d4f68678768

18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed

Severity
High

Description

Description The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Rationale EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows

Recommendation
Install EMET 5.5 or higher.

Failed Instances
i-03e085d4f68678768

18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)

Severity
High

Description
Description This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation Settings - EnabledDeep Hooks - EnabledAnti Detours - EnabledBanned Functions - EnabledExploit Action - User Configured Rationale These advanced mitigations for ROP mitigations apply to all configured software in EMET. Deep Hooks protects critical APIs and the subsequent lower level APIs used by the top level critical API. Anti Detours renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue. Banned Functions will block calls to ntdll!LdrHotPatchRoutine to mitigate potential exploits abusing the API.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to Internet Explorer. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Internet Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to other popular software. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'

Severity
High

Description
Description This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In. Rationale ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-In: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System ASLR Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System DEP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP). The recommended state for this

setting is: Enabled: Application Opt-Out. Rationale When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System SEHOP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates

\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that

uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 196,608 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes)

in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure

this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrativ

e Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Severity
High

Description
Description Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled. Rationale Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer Impact: Enabling this policy setting may allow certain legacy plug-in applications to function. Disabling this policy setting will ensure that Data Execution Prevention blocks certain types of malware from exploiting Explorer.

Failed Instances
i-03e085d4f68678768

18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Severity
High

Description
Description Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled. Rationale Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off heap termination on corruption Impact: Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately although Explorer may still terminate unexpectedly later.

Failed Instances
i-03e085d4f68678768

18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled. Rationale

Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off shell protocol protected mode Impact: If you enable this policy setting the protocol is fully enabled allowing the opening of folders and files. If you disable this policy setting the protocol is in the protected mode allowing applications to only open a limited set of folders.

Failed Instances
i-03e085d4f68678768

18.9.35.1 (L2) Ensure 'Turn off location' is set to 'Enabled'

Severity
High

Description
Description This policy setting turns off the location feature for this computer. The recommended state for this setting is: Enabled. Rationale This setting affects the location feature (e.g. GPS or other location tracking). From a security perspective, it#x2019;s not a good idea to reveal your location to software in most cases, but there are legitimate uses, such as mapping software.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\Turn off location Impact: If you enable this policy setting, the location feature is turned off, and all programs on this computer are prevented from using location information from the location feature.

Failed Instances
i-03e085d4f68678768

18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Severity
High

Description

Description This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server. The recommended state for this setting is: Enabled. Rationale An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Recommendation

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Connection Client \Do not allow passwords to be saved Impact: If you enable this policy setting, the password saving checkbox is disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Failed Instances

i-03e085d4f68678768

18.9.48.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'

Severity

High

Description

Description This policy setting allows you to restrict users to a single Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale This setting ensures that users & administrators who Remote Desktop to a server will continue to use the same session - if they disconnect and reconnect, they will go back to the same session they were using before, preventing the creation of a second simultaneous session. This both prevents unnecessary resource usage by having the server host unnecessary additional sessions (which would put extra load on the server) and also ensures a consistency of experience for the user.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections \Restrict Remote Desktop Services users to a single Remote Desktop Services session Impact: If you enable this policy setting, users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.If you disable this policy setting, users are allowed to make unlimited simultaneous remote connections by using Remote Desktop Services.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for COM port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection Impact: If you enable this policy setting, users cannot redirect server data to the local COM port.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient \<driveletter>$ If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled. Rationale Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection Impact: Drive redirection will not be possible. In most cases, traditional network drive mapping to file shares (including administrative shares) will serve as a capable substitute to still allow file transfers when needed.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for LPT port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection Impact: If you enable this policy setting, users in a Remote Desktop Services session cannot redirect server data to the local LPT port.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for Plug and Play device redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow supported Plug and Play device redirection Impact: If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client. Note: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent. The recommended state for this setting is: Enabled. Rationale Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection Impact: Users will always have to enter their password when they establish new Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC

communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled. Rationale Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication Impact: If you enable this policy setting, the terminal server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Severity
High

Description
Description This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. The recommended state for this setting is Enabled: High Level. Rationale If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: High Level: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Security\Set client connection encryption level Impact: Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'

Severity
High

Description
Description This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected. The recommended state for this setting is: Enabled: 15 minutes or less. Rationale This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of inactive sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 15 minutes or less: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for active but idle Remote Desktop Services sessions Impact: If you enable this policy setting, you must select the desired time limit in the Idle session limit list. Remote Desktop Services will automatically disconnect active but idle sessions after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply.

Failed Instances
i-03e085d4f68678768

18.9.48.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. The recommended state for this setting is: Enabled: 1 minute. Rationale This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of disconnected but still active sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service. This setting is important to ensure a disconnected session is properly terminated.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Session Time Limits\Set time limit for disconnected sessions Impact: If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled. Rationale Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Do not delete temp folders upon exit Impact: If you disable this policy setting, temporary folders are deleted when a user logs off, even if the server administrator specifies otherwise.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Severity
High

Description
Description By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled. Rationale By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session Impact: If this setting is enabled, only one temporary folder is used for all remote sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Failed Instances
i-03e085d4f68678768

18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled. Rationale Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures Impact: If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.

Failed Instances
i-03e085d4f68678768

18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled. Rationale Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: The search service components (including non-Microsoft components) will not encrypted items or encrypted stores.

Failed Instances
i-03e085d4f68678768

18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'

Severity
High

Description
Description This setting allows you to set the default consent handling for error reports. The recommended state for this setting is: Enabled: Always ask before sending data Rationale Error reports may contain sensitive information and should not be sent to anyone automatically.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Always ask before sending data: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\Configure Default consent Impact: By setting to always ask before sending data: Windows prompts users for consent to send reports.

Failed Instances
i-03e085d4f68678768

18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Severity
High

Description
Description Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled. Rationale In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs Impact: If you disable or do not configure this policy setting, the security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.

Failed Instances
i-03e085d4f68678768

18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Severity
High

Description
Description Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs

programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled. Rationale Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

Failed Instances
i-03e085d4f68678768

18.9.69.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows Web-based programs to install software on the computer without notifying the user. The recommended state for this setting is: Disabled. Rationale Suppressing the system warning can pose a security risk and increase the attack surface on the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows

Installer scripts Impact: If you disable or do not configure this policy setting by default when a script hosted by an Internet browser tries to install a program on the system the system warns users and allows them to select or refuse the installation. If you enable this policy setting the warning is suppressed and allows the installation to proceed. This policy setting is designed for enterprises that use Web-based tools to distribute programs to their employees. However because this policy setting can pose a security risk it should be applied cautiously.

Failed Instances
i-03e085d4f68678768

18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for this setting is: Disabled. Rationale Due to the potential risks of capturing passwords in the logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, logging of PowerShell script input is disabled.

Failed Instances
i-03e085d4f68678768

18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Severity
High

Description
Description This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled. Rationale If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Transcription Note: This Group Policy path does not exist by default. A newer version of the "powershelle xecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the Start-Transcript cmdlet.

Failed Instances
i-03e085d4f68678768

18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication. The

recommended state for this setting is: Enabled. Rationale Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication Impact: The WinRM client will not use Digest authentication.

Failed Instances
i-03e085d4f68678768

18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins

and the RunAsPassword value will be stored securely. If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset. The recommended state for this setting is: Enabled. Rationale Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer.If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Failed Instances
i-03e085d4f68678768

18.9.82.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands. The recommended state for this setting is: Disabled. Rationale Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Shell on trusted networks and when feasible employ additional controls such as IPsec.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled. Computer Configuration\Administrative Templates\Windows

Components\Windows Remote Shell\Allow Remote Shell Access Impact: If you disable or do not configure this policy setting, remote access is not allowed to all supported shells to execute scripts and commands.

Failed Instances
i-03e085d4f68678768

18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: Enabled. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances

i-03e085d4f68678768

18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: 0 - Every day. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 0 - Every day: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. The recommended state for this setting is: Disabled. Rationale Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Administrative Templates\Windows Components \Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is displayed in the Shut Down Windows dialog box. The recommended state for this setting is: Disabled. Rationale Alerting users that a system needs to be patch is a good way to help ensure patching is being applied to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows

Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be available in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are:- Enabled- Disabled- Not Configured Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: Disabled. Rationale Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled

automatic updates installations Impact: If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

Failed Instances
i-03e085d4f68678768

18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. The recommended state for this setting is: Enabled: 1 minute. Rationale Rescheduling automatic updates that were not installed on schedule will help ensure security patches get installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations Impact: Remaining Automatic Updates will start 1 minute after the computer restarts.

Failed Instances
i-03e085d4f68678768

4.1.4 Level 2 - Member Server

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Severity
High

Description
Description This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value

for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s). Rationale The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Failed Instances
i-03e085d4f68678768

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'

Severity
High

Description
Description This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is

between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s). Rationale Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings \Account Policies\Password Policy\Minimum password age Impact: If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Failed Instances
i-03e085d4f68678768

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Severity
High

Description
Description This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be

educated about the proper selection and maintenance of passwords, especially with regard to password length.In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Rationale Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Failed Instances
i-03e085d4f68678768

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Severity
High

Description
Description This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0. Rationale Setting an account lockout threshold reduces the likelihood that an online password brute force attack will

be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Failed Instances
i-03e085d4f68678768

2.2.2 (L1) Configure 'Access this computer from the network'

Severity
High

Description
Description This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators, Authenticated Users. Rationale Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not

include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Access this computer from the network Impact: If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore it is recommended that it is assigned to the Users group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Failed Instances
i-03e085d4f68678768

2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network

applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE: Computer Configuration \Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment \Adjust memory quotas for a process Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Failed Instances
i-03e085d4f68678768

2.2.6 (L1) Configure 'Allow log on locally'

Severity
High

Description
Description This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT +DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, ENTERPRISE DOMAIN CONTROLLERS.Level 1 - Member Server. The recommended state for this setting is: Administrators. Rationale Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \User Rights Assignment\Allow log on locally Impact: If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

Failed Instances
i-03e085d4f68678768

2.2.8 (L1) Ensure 'Back up files and directories' is set to 'Administrators'

Severity
High

Description
Description This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators. Rationale Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Back up files and directories Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Failed Instances
i-03e085d4f68678768

2.2.18 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'

Severity
High

Description
Description This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests. Rationale Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a batch job Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Failed Instances
i-03e085d4f68678768

2.2.19 (L1) Ensure 'Deny log on as a service' to include 'Guests'

Severity
High

Description

Description This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests. Note: This security setting does not apply to the System, Local Service, or Network Service accounts. Rationale Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on as a service Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Failed Instances

i-03e085d4f68678768

2.2.20 (L1) Ensure 'Deny log on locally' to include 'Guests'

Severity

High

Description

Description This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests. Rationale Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Deny log on locally Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Severity
High

Description
Description This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account. Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server. Rationale Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Recommendation
To establish the recommended configuration via GP, set the following UI path to include Guests, Local account: Computer Configuration\Policies\Windows Settings \Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Failed Instances
i-03e085d4f68678768

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Severity
High

Description
Description This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right. Rationale User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

Recommendation
To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies \Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Failed Instances
i-03e085d4f68678768

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Severity
High

Description

Description This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. Rationale An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Failed Instances

i-03e085d4f68678768

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators'

Severity

High

Description

Description This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators. Rationale The ability to

shut down domain controllers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords#x2014;the Primary Domain Controller (PDC) Emulator role.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\User Rights Assignment\Shut down the system Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Failed Instances
i-03e085d4f68678768

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'

Severity
High

Description
Description This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled. Rationale In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a

prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Failed Instances
i-03e085d4f68678768

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'

Severity
High

Description
Description The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). Rationale The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account

has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename administrator account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Failed Instances
i-03e085d4f68678768

2.3.1.5 (L1) Configure 'Accounts: Rename guest account'

Severity
High

Description
Description The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. Rationale The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Recommendation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

Failed Instances
i-03e085d4f68678768

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled. Rationale Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Failed Instances
i-03e085d4f68678768

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Severity
High

Description
Description This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators. Rationale Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default value. Only Administrators will be able to format and eject removable NTFS media.

Failed Instances
i-03e085d4f68678768

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled. Rationale An attacker with access to the console (for example, someone with physical access or

someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

Failed Instances
i-03e085d4f68678768

2.3.7.3 (L1) Configure 'Interactive logon: Message text for users attempting to log on'

Severity
High

Description
Description This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons#x2014;for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Recommendation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message text for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain

carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances
i-03e085d4f68678768

2.3.7.4 (L1) Configure 'Interactive logon: Message title for users attempting to log on'

Severity
High

Description
Description This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization. Rationale Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Recommendation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Message title for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you

inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Failed Instances
i-03e085d4f68678768

2.3.7.5 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only)

Severity
High

Description
Description This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: 4 or fewer logon(s). Rationale The number that is assigned to this policy setting indicates the number of users whose logon information the servers will cache locally. If the number is set to 10, then the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session. Users who access the server console will have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to attempt to determine user passwords.To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 4 or fewer logon(s): Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Interactive logon: Number of previous logons to cache

(in case domain controller is not available) Impact: Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Failed Instances
i-03e085d4f68678768

2.3.7.7 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)

Severity
High

Description
Description Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. The recommended state for this setting is: Enabled. Rationale By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account#x2014;such as user rights assignments, account lockout, or the account being disabled#x2014;are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

Recommendation
To implement the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local

Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation Impact: When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.

Failed Instances
i-03e085d4f68678768

2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Severity
High

Description
Description This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark. Rationale Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior Impact: If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several

computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Failed Instances
i-03e085d4f68678768

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools

that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances

i-03e085d4f68678768

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled. Rationale Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be

substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Failed Instances
i-03e085d4f68678768

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Severity
High

Description
Description This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms with the benchmark. Rationale The identity of a computer can be spoofed to gain unauthorized access to network resources.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms with

the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Microsoft network server: Server SPN target name validation level Impact: All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Failed Instances
i-03e085d4f68678768

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: Disabled. Rationale If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003-based domains. For example, the following computers may not work:Windows NT 4.0-based Remote Access Service servers.Microsoft SQL Servers#x2122; that run on Windows NT 3.x-based or Windows NT 4.0-based computers.Remote Access Service or Microsoft SQL servers that run on Windows 2000-based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Failed Instances
i-03e085d4f68678768

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting is: Enabled. Rationale An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares Impact: It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Failed Instances
i-03e085d4f68678768

2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether the Stored User Names and Passwords feature may save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the Stored User Names and Passwords feature of Windows does not store passwords and credentials. The recommended state for this setting is: Enabled. Rationale Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication Impact: Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Failed Instances
i-03e085d4f68678768

2.3.10.10 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Severity
High

Description
Description This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None). Rationale It is

very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously Impact: There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

Failed Instances
i-03e085d4f68678768

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Severity
High

Description
Description When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled. Rationale When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer

identity for NTLM Impact: If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Failed Instances
i-03e085d4f68678768

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Severity
High

Description
Description Allow NTLM to fall back to NULL session when used with LocalSystem. The default is TRUE up to Windows Vista / Server 2008 and FALSE from Windows 7 / Server 2008 R2 and beyond. The recommended state for this setting is: Disabled. Rationale NULL sessions are less secure because by definition they are unauthenticated.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Failed Instances
i-03e085d4f68678768

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

Severity
High

Description

Description This setting determines if online identities are able to authenticate to this computer. Windows 7 and Windows Server 2008 R2 introduced an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled. Rationale The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities Impact: Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7 and later.

Failed Instances
i-03e085d4f68678768

2.3.11.4 (L1) Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Severity
High

Description
Description This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types. Rationale The strength of each encryption algorithm varies from one to the next, choosing

stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings \Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos Impact: If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Failed Instances
i-03e085d4f68678768

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

Severity
High

Description
Description LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: Join a domainAuthenticate between Active Directory forestsAuthenticate to down-level domainsAuthenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: Send LM & NTLM responsesSend LM & NTLM #x2014; use NTLMv2 session security if negotiatedSend NTLM responses onlySend NTLMv2 responses onlySend NTLMv2 responses only\refuse LMSend NTLMv2 responses only\refuse LM & NTLMNot Defined The Network

security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send LM & NTLM - use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).These settings correspond to the levels discussed in other Microsoft documents as follows:Level 0 - Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 1 - Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 3 - Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2.Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state

for this setting is: Send NTLMv2 response only. Refuse LM & NTLM. Rationale
In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses#x2014;the weakest form of authentication response#x2014;are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level Impact: Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Failed Instances
i-03e085d4f68678768

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity

High

Description

Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Impact: Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use

NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Severity
High

Description
Description This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Rationale You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Recommendation

To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Impact: Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Failed Instances
i-03e085d4f68678768

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)'

Severity
High

Description
Description This security setting determines which subsystems can optionally be started up to support your applications. The recommended state for this setting is: Defined: (blank) Rationale Leaving POSIX enabled could introduce an additional attack surface in your environment.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Defined: (blank) : Computer Configuration\Security Settings\Local Policies\Security Options\System settings: Optional subsystems Impact: Removes POSIX compatibility.

Failed Instances
i-03e085d4f68678768

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

Severity

High

Description

Description This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: Enabled. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account Impact: Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Failed Instances

i-03e085d4f68678768

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Severity

High

Description

Description This policy setting controls the behavior of the elevation prompt for administrators. The options are:- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.- Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.- Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: Prompt for consent on the secure desktop. Rationale One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Impact: This policy setting controls the behavior of the elevation prompt for administrators.

Failed Instances

i-03e085d4f68678768

2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Severity
High

Description
Description This policy setting controls the behavior of the elevation prompt for standard users. The options are: Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: Automatically deny elevation requests. Rationale One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users Impact: Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Failed Instances
i-03e085d4f68678768

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system

then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista / Server 2008 and above, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: Allow (default). Rationale Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group

Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances

i-03e085d4f68678768

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security

\Windows Firewall Properties\Private Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound

connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale
Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No. Rationale Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default). Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\privatefw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYS TEMROOT%\System32\logfiles\firewall\privatefw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced

Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Private Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.2.9 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet

was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.2.10 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Severity
High

Description
Description Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended). Rationale If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Firewall state Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Severity
High

Description
Description This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default). Rationale If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Inbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Severity
High

Description
Description This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default). Rationale
Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security \Windows Firewall Properties\Public Profile\Outbound connections Impact: None, this is the default configuration.

Failed Instances
i-03e085d4f68678768

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'

Severity
High

Description
Description Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: Yes. Rationale Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Failed Instances
i-03e085d4f68678768

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Severity
High

Description

Description This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No. Rationale When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Severity
High

Description
Description This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No. Rationale Users with administrative privileges might create firewall rules that expose the system to remote attack.

Recommendation
To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Failed Instances
i-03e085d4f68678768

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEM ROOT%\System32\logfiles\firewall\publicfw.log'

Severity
High

Description
Description Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log: Computer Configuration \Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties \Public Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Failed Instances
i-03e085d4f68678768

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Severity
High

Description
Description Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Failed Instances
i-03e085d4f68678768

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Severity
High

Description
Description Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Severity

High

Description
Description Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Failed Instances
i-03e085d4f68678768

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon.4775: An account could not be mapped for logon.4776: The domain controller attempted to validate the credentials for an account.4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is:

Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Severity
High

Description
Description This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted.Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security

Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Application Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created.4742: A computer account was changed.4743: A computer account was deleted. The recommended state for this setting is: Success and Failure. Rationale Auditing events in this category may be useful when investigating an incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Computer Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed.4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Other Account Management Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.5 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure'

Severity
High

Description

Description This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created.4728: A member was added to a security-enabled global group.4729: A member was removed from a security-enabled global group.4730: A security-enabled global group was deleted.4731: A security-enabled local group was created.4732: A member was added to a security-enabled local group.4733: A member was removed from a security-enabled local group.4734: A security-enabled local group was deleted.4735: A security-enabled local group was changed.4737: A security-enabled global group was changed.4754: A security-enabled universal group was created.4755: A security-enabled universal group was changed.4756: A member was added to a security-enabled universal group.4757: A member was removed from a security-enabled universal group.4758: A security-enabled universal group was deleted.4764: A group's type was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit Security Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Severity

High

Description

Description This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created.4722: A user account was enabled.4723: An attempt was made to change an account's password.4724: An attempt was made to reset an account's password.4725: A user account was disabled.4726: A user account was deleted.4738: A user account was changed.4740: A user account was locked out.4765: SID History was added to an account.4766: An attempt to add SID History to an account failed.4767: A user account was unlocked.4780: The ACL was set on accounts which are members of administrators groups.4781: The name of an account was changed:4794: An attempt was made to set the Directory Services Restore Mode.5376: Credential Manager credentials were backed up.5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management \Audit User Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances

i-03e085d4f68678768

17.3.1 (L1) Ensure 'Audit Process Creation' is set to 'Success'

Severity

High

Description
Description This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created.4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings \Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected.4778: A session was reconnected to a Window Station.4779: A session was disconnected from a Window Station.4800: The workstation was locked.4801: The workstation was unlocked.4802:

The screen saver was invoked.4803: The screen saver was dismissed.5378: The requested credentials delegation was disallowed by policy.5632: A request was made to authenticate to a wireless network.5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed.4719: System audit policy was changed.4902: The Per-user audit policy table was created.4904: An attempt was made to register a security event source.4905: An attempt was made to unregister a security event source.4906: The CrashOnAuditFail value has changed.4907: Auditing settings on object were changed.4908: Special Groups Logon table modified.4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use Impact: If no audit settings are configured, or if audit settings

are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.5478: IPsec Services has started successfully.5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5480: IPsec Services failed to get

the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure'

Severity
High

Description
Description This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority.4611: A trusted logon process has been registered with the Local Security Authority.4614: A notification package has been loaded by the Security Account Manager.4622: A security

package has been loaded by the Local Security Authority.4697: A service was installed in the system. The recommended state for this setting is: Success and Failure. Rationale Auditing these events may be useful when investigating a security incident.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Failed Instances
i-03e085d4f68678768

18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the

difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file AdmPwd.dll must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you): C:\Program Files\LAPS\CSE\AdmPwd.dll Impact: No impact. When installed and registered properly, AdmPwd.dll takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service.In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Failed Instances
i-03e085d4f68678768

18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation

OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: When you enable this setting, planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Failed Instances
i-03e085d4f68678768

18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the

LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: If you enable this setting, local administrator password is managed. If you disable or not configure this setting, local administrator password is NOT managed.In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Failed Instances
i-03e085d4f68678768

18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in

a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexity option to Large letters + small letters + numbers + special characters : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires password to contain large letters + small letters + numbers + special characters

Failed Instances
i-03e085d4f68678768

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords

on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 15 or more. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Length option to 15 or more : Computer Conf iguration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires the password to have a length of a minimum of 15 characters .

Failed Instances
i-03e085d4f68678768

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)

Severity
High

Description
Description In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization

to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 30 or fewer. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Rationale Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Age (Days) option to 30 or fewer : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires a maximum password age of 30 days or less.

Failed Instances
i-03e085d4f68678768

18.3.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Severity
High

Description

Description This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled. Rationale If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None. By default this entry is not enabled.

Failed Instances
i-03e085d4f68678768

18.3.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configur ation\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Severity
High

Description
Description IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Rationale An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet

spoofing) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: All incoming source routed packets will be dropped.

Failed Instances
i-03e085d4f68678768

18.3.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Severity
High

Description
Description Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled. Rationale This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Failed Instances
i-03e085d4f68678768

18.3.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'

Severity
High

Description
Description This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet. The recommended state for this setting is: Enabled: 300,000 or 5 minutes (recommended). Rationale An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 300,000 or 5 minutes (recommended) : Computer Configuration\Policies \Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Failed Instances
i-03e085d4f68678768

18.3.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Severity
High

Description
Description NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting

determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled. Rationale The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Failed Instances
i-03e085d4f68678768

18.3.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'

Severity
High

Description
Description This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis. The recommended state for this setting is: Disabled. Rationale An attacker who has gained control of a computer on the same network segment could configure a computer on

the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: If you disable this entry, Windows Server 2003 (which supports the IRDP) cannot automatically detect and configure default gateway addresses on the computer.

Failed Instances
i-03e085d4f68678768

18.3.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Severity
High

Description
Description The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the system path first, and then search the current working folder.Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: Enabled. Rationale If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS

(Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Failed Instances
i-03e085d4f68678768

18.3.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Severity
High

Description
Description Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds. Rationale The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Failed Instances

i-03e085d4f68678768

18.3.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Severity
High

Description
Description This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3. Rationale A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 3: Computer Configuration\Policies\Administrative Templates\MSS (Legacy) \MSS:(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Failed Instances
i-03e085d4f68678768

18.3.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Severity
High

Description

Description This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3. Rationale A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 3: Computer Configuration\Policies\Administrative Templates\MSS (Leg acy)\MSS:(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Failed Instances
i-03e085d4f68678768

18.3.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Severity
High

Description
Description This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less. Rationale If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less: Computer Configuration\Policies\Administrative Templates \MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

Failed Instances
i-03e085d4f68678768

18.4.8.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'

Severity
High

Description
Description This policy setting changes the operational behavior of the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Rationale To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver Impact: If you disable or do not configure this policy setting, the default behavior of LLTDIO will apply.

Failed Instances
i-03e085d4f68678768

18.4.8.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'

Severity
High

Description
Description This policy setting changes the operational behavior of the Responder network protocol driver. The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Rationale To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver Impact: If you disable or do not configure this policy setting, the default behavior of RSPNDR will apply.

Failed Instances
i-03e085d4f68678768

18.4.9.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'

Severity
High

Description
Description The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPV6 address and port number. The protocol operates in the context of clouds . A cloud is a set of peer computers that can communicate with each other by using the same IPv6 scope. Peer-to-Peer protocols allow for applications in the areas of RTC, collaboration, content distribution and distributed processing. The recommended state for this setting is: Enabled. Rationale This setting enhances the security of the environment and reduces the overall risk exposure related to peer-to-peer networking.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Microsoft Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking Services Impact: If you enable this setting, peer-to-peer protocols will be turned off. If you disable this setting or do not configure it, the peer-to-peer protocols will be turned on. This setting turns off Microsoft Peer-to-Peer Networking Services in its entirety, and will cause all dependent applications to stop working.

Failed Instances
i-03e085d4f68678768

18.4.10.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Severity
High

Description
Description You can use this procedure to enable or disable the user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled. Rationale Allowing users to create a network bridge increases the risk and attack surface from the bridged network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network Impact: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, you can disable the Network Bridge setting on a computer. If you disable Network Bridge on a computer, users cannot create or configure a network bridge. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

Failed Instances

i-03e085d4f68678768

18.4.10.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'

Severity
High

Description
Description This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled. Rationale Allowing regular users to set a network location increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network \Network Connections\Require domain users to elevate when setting a network's location Impact: If you enable this policy setting domain users must elevate when setting a network's location. If you disable or do not configure this policy setting domain users can set a network's location without elevating.

Failed Instances
i-03e085d4f68678768

18.4.13.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Severity
High

Description
Description This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares. Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough

testing. Rationale In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Failed Instances
i-03e085d4f68678768

18.4.18.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')

Severity
High

Description
Description Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6

allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively. The recommended state for this setting is: DisabledComponents - 0xff (255) Rationale Since the vast majority of private corporate networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling IPv6 components reduces a possible attack surface that is also harder to monitor the traffic on. As a result, we recommend configuring IPv6 to a Disabled state when it is not needed.

Recommendation
To establish the recommended configuration, set the following Registry value to 0xff (255) (DWORD): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TCPIP6\Parameters:DisabledComponents Note: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (Disable -IPv6-Components-KB929852.adm) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state. Impact: Connectivity to other systems using IPv6 will no longer operate, and software that depends on IPv6 will cease to function. Examples of Microsoft applications that may use IPv6 include: Remote Assistance, HomeGroup, DirectAccess, Windows Mail.This registry change is documented in Microsoft Knowledge Base article 929852: How to disable IPv6 or its components in Windows.Note: This registry change does not take effect until the next reboot.

Failed Instances
i-03e085d4f68678768

18.4.19.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over In-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium.

The recommended state for this setting is: Disabled. Rationale This setting enhances the security of the environment and reduces the overall risk exposure related to user configuration of wireless settings.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Network \Windows Connect Now\Configuration of wireless settings using Windows Connect Now Impact: If you enable this policy setting additional choices are available to turn off the operations over a specific medium. If you disable this policy setting operations are disabled over all media. If you do not configure this policy setting operations are enabled over all media.

Failed Instances
i-03e085d4f68678768

18.4.19.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'

Severity
High

Description
Description This policy setting prohibits access to Windows Connect Now (WCN) wizards. The recommended state for this setting is: Enabled. Rationale Allowing standard users to access the Windows Connect Now wizard increases the risk and attack surface.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Network\Network \Windows Connect Now\Prohibit access of the Windows Connect Now wizards Impact: If you enable this policy setting the wizards are turned off and users have no access to any of the wizard tasks. All the configuration related tasks including "Set up a wireless router or access point" and "Add a wireless device" are disabled. If you disable or do not configure this policy setting users can access the wizard tasks including "Set up a wireless router or access point" and "Add a wireless device."

Failed Instances

i-03e085d4f68678768

18.6.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)

Severity
High

Description
Description This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk. Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the LocalAccountTokenFilterPolicy registry value to 0. This is the default behavior for Windows. Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about LocalAccountTokenFilterPolicy, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista. The recommended state for this setting is: Enabled. Rationale Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\Apply UAC restrictions to local accounts on network logons Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.6.2 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Severity
High

Description
Description When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is: Disabled. Rationale Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997) Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: None - this is the default behavior for Windows 8.1 and Server 2012 R2.

Failed Instances
i-03e085d4f68678768

18.8.2.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'

Severity
High

Description
Description This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is:

Disabled. Rationale When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Impact: If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

Failed Instances
i-03e085d4f68678768

18.8.5.2 (L1) Ensure 'Allow remote access to the Plug and Play interface' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to allow or deny remote access to the Plug and Play interface. The recommended state for this setting is: Disabled. Rationale Allowing remote access to the Plug and Play interface could give hackers another attack vector to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow remote access to the Plug and Play interface Impact: If you disable or do not configure this policy setting, remote connections to the Plug and Play interface are not allowed.

Failed Instances
i-03e085d4f68678768

18.8.18.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'

Severity
High

Description
Description The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked). Rationale Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.18.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Severity
High

Description
Description The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked). Rationale Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option

to TRUE (checked): Computer Configuration\Policies\Administrative Templates \System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Failed Instances
i-03e085d4f68678768

18.8.19.1.1 (L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP. The recommended state for this setting is: Enabled. Rationale Users might download drivers that include malicious code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP Impact: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits drivers that are not already installed locally from downloading.

Failed Instances
i-03e085d4f68678768

18.8.19.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'

Severity
High

Description

Description This setting turns off data sharing from the handwriting recognition personalization tool. The handwriting recognition personalization tool enables Tablet PC users to adapt handwriting recognition to their own writing style by providing writing samples. The tool can optionally share user writing samples with Microsoft to improve handwriting recognition in future versions of Windows. The tool generates reports and transmits them to Microsoft over a secure connection. The recommended state for this setting is: Enabled. Rationale A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting personalization data sharing Note: This Group Policy setting is provided by the Group Policy template "ShapeCollector.admx/adml" that is included with the Microsoft Windows 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: If you enable this policy, Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

Failed Instances
i-03e085d4f68678768

18.8.19.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'

Severity
High

Description
Description Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. The recommended state for this setting is: Enabled. Rationale A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many

environments to automatically upload PII to a website without explicit approval by the user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting recognition error reporting Impact: If you enable this policy, users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

Failed Instances
i-03e085d4f68678768

18.8.19.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs). The recommended state for this setting is: Enabled. Rationale In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com Impact: If you enable this policy setting, the "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

Failed Instances
i-03e085d4f68678768

18.8.19.1.5 (L2) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards. The recommended state for this setting is: Enabled. Rationale Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards Impact: If this policy setting is enabled, Windows is prevented from downloading providers; only the service providers cached in the local registry will display.

Failed Instances
i-03e085d4f68678768

18.8.19.1.6 (L2) Ensure 'Turn off Internet File Association service' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to use the Microsoft Web service for finding an application to open a file with an unhandled file association. When a user opens a file that has an extension that is not associated with any applications on the computer, the user is given the choice to select a local application or use the Web service to find an application. The recommended state for this setting is: Enabled. Rationale This service#x2019;s purpose is to help find an appropriate application for a file whose type is unrecognized by the computer. That could pose a security risk if the unrecognized file is malicious code, even if the application to be discovered is itself innocent. Corporate environments tend to be very managed, where the IT staff decide which applications should and should not be installed.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet File Association service Impact: If you enable this policy setting, the link and the dialog for using the Web service to open an unhandled file association are removed.

Failed Instances
i-03e085d4f68678768

18.8.19.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet. The recommended state for this setting is: Enabled. Rationale Information that is transmitted over HTTP through this capability is not protected and can be intercepted by malicious users. For this reason, it is not often used in enterprise environments.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP Impact: If you enable this policy setting, the client computer will not be able to print to Internet printers over HTTP. This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

Failed Instances
i-03e085d4f68678768

18.8.19.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration. The recommended state for this setting is: Enabled. Rationale Users in a corporate environment should not be registering their own copies of Windows, providing their own PII in the process.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registration if URL connection is referring to Microsoft.com Impact: If you enable this policy setting, it blocks users from connecting to Microsoft.com for online registration and users cannot register their copy of Windows online.

Failed Instances
i-03e085d4f68678768

18.8.19.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches. The recommended state for this setting is: Enabled. Rationale There is a small risk that users will unknowingly reveal sensitive information because of the topics they are searching for. This risk is very low because even if this setting is enabled users still must submit search queries to the desired search engine in order to perform searches.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates Impact: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select

Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.

Failed Instances
i-03e085d4f68678768

18.8.19.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the "Order Prints Online" task is available from Picture Tasks in Windows folders. The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online. The recommended state for this setting is: Enabled. Rationale In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task Impact: If you enable this policy setting, the task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Failed Instances
i-03e085d4f68678768

18.8.19.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web are available from File and Folder Tasks in Windows folders. The recommended state for this setting is: Enabled. Rationale Users may publish confidential or sensitive information to a public service outside of the control of the organization.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders Impact: The Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.

Failed Instances
i-03e085d4f68678768

18.8.19.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. The recommended state for this setting is: Enabled. Rationale Large enterprise environments may not want to have information collected from managed client computers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program Impact: Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

Failed Instances
i-03e085d4f68678768

18.8.19.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

Severity

High

Description
Description This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. The recommended state for this setting is: Enabled. Rationale Large enterprise environments may not want to have information collected from managed client computers.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program Impact: Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

Failed Instances
i-03e085d4f68678768

18.8.19.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'

Severity
High

Description
Description This policy setting controls whether or not errors are reported to Microsoft. Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product. The recommended state for this setting is: Enabled. Rationale If a Windows Error occurs in a secure, managed corporate environment, the error should be reported directly to IT staff for troubleshooting and remediation. There is no benefit to the corporation to report these errors directly to Microsoft, and there is some risk of unknowingly exposing sensitive data as part of the error.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet

Communication Management\Internet Communication settings\Turn off Windows Error Reporting Impact: If you enable this policy setting, users are not given the option to report errors.

Failed Instances
i-03e085d4f68678768

18.8.24.1 (L1) Ensure 'Always use classic logon' is set to 'Enabled'

Severity
High

Description
Description This policy setting forces the user to log on to the computer using the classic logon screen. By default, a workgroup is set to use the simple logon screen. This setting only works when the computer is not on a domain. The recommended state for this setting is: Enabled. Rationale Explicitly requiring a user to enter their username and password is ideal and a requirement when utilizing the classic logon method. This setting is primarily important because it does not permit the use of a simple logon screen with user accounts presented. (Note: Systems joined to a domain typically are not impacted by this recommendation as username, password, and domain are required for system access. However, this setting is important for standalone systems.)

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Administrative Templates\System\Logon\Always use classic logon Impact: If you enable this policy setting, the classic logon screen is presented to the user at logon, rather than the simple logon screen.

Failed Instances
i-03e085d4f68678768

18.8.28.4.1 (L2) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

Severity
High

Description

Description Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled. Rationale Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery) Impact: If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep.If you disable this policy, the user is not prompted for a password when the system resumes from sleep.

Failed Instances
i-03e085d4f68678768

18.8.28.4.2 (L2) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

Severity
High

Description
Description Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled. Rationale Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in) Impact: If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep.If you disable this policy, the user is not prompted for a password when the system resumes from sleep.

Failed Instances

i-03e085d4f68678768

18.8.30.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. If you enable this policy setting, users on this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance. To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:<Domain Name>\<User Name> or<Domain Name>\<Group Name> If you enable this policy setting, you should also enable firewall exceptions to allow Remote Assistance communications. The firewall exceptions required for Offer (Unsolicited) Remote Assistance depend on the version of Windows you are running: Windows Vista and later:Enable the Remote Assistance exception for the domain profile. The exception must contain:Port 135:TCP%WINDIR%\System32\msra.exe%WINDIR%\System32\raserver.exe Windows XP with Service Pack 2 (SP2) and Windows XP Professional x64 Edition with Service Pack 1 (SP1):Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe%WINDIR%\System32\Sessmgr.exe For computers running Windows Server 2003 with Service Pack 1 (SP1)Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exeAllow Remote Desktop Exception The recommended state for this setting is: Disabled. Rationale A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance Impact: Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Failed Instances
i-03e085d4f68678768

18.8.30.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open. The "Select the method for sending email invitations" setting specifies which email standard to use to send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your email message). This policy setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy setting you should also enable appropriate firewall exceptions to allow Remote Assistance communications. The recommended state for this setting is: Disabled. Rationale There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's

computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance Impact: If you enable this policy, users on this computer can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings.If you disable this policy, users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

Failed Instances
i-03e085d4f68678768

18.8.31.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)

Severity
High

Description
Description This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the trusting domain DCs (see Microsoft KB3073942), so we do not recommend applying it to domain controllers. If you disable this policy setting, RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Endpoint Mapper Service on Windows NT4 Server. If you enable this policy setting, RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to

communicate with the Windows NT4 Server Endpoint Mapper Service. If you do not configure this policy setting, it remains disabled. RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service. Note: This policy will not be applied until the system is rebooted. The recommended state for this setting is: Enabled. Rationale Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System \Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication Impact: RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Failed Instances
i-03e085d4f68678768

18.8.31.2 (L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only)

Severity
High

Description
Description This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers. This policy setting impacts all RPC applications. In a domain environment this policy setting should be used with caution as it can impact a wide range of functionality including group policy processing itself. Reverting a change to this policy setting can require manual intervention on each affected machine. This policy setting should never be applied to a domain controller. If you disable this policy setting, the RPC server runtime uses the value of "Authenticated" on Windows Client, and the value of "None" on Windows Server versions that support this policy setting. If you do not configure this policy setting, it remains disabled. The RPC server runtime will behave as though it was enabled with the value of "Authenticated" used for Windows Client and the value of "None" used for Server SKUs that support this policy setting. If you enable this policy setting, it directs the RPC server runtime to restrict unauthenticated RPC clients connecting to

RPC servers running on a machine. A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically requested to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy setting. -- "None" allows all RPC clients to connect to RPC Servers running on the machine on which the policy setting is applied.-- "Authenticated" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.-- "Authenticated without exceptions" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. No exceptions are allowed. This value has the potential to cause serious problems and is not recommended. Note: This policy setting will not be applied until the system is rebooted. The recommended state for this setting is: Enabled: Authenticated. Rationale Unauthenticated RPC communication can create a security vulnerability.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Authenticated: Computer Configuration\Policies\Administrative Templates \System\Remote Procedure Call\Restrict Unauthenticated RPC clients Impact: Only authenticated RPC Clients will be allowed to connect to RPC Servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.

Failed Instances
i-03e085d4f68678768

18.8.38.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'

Severity
High

Description
Description This policy setting configures Microsoft Support Diagnostic Tool (MSDT) interactive communication with the support provider. MSDT gathers diagnostic data for analysis by support professionals. The recommended state for this setting is: Disabled. Rationale Due to privacy concerns, data should never be sent to any 3rd party since this data could contain sensitive information.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Tro ubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider Impact: If you disable this policy setting, MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Failed Instances
i-03e085d4f68678768

18.8.38.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether to enable or disable tracking of responsiveness events. The recommended state for this setting is: Disabled. Rationale When enabled the aggregated data of a given event will be transmitted to Microsoft. The option exists to restrict this feature for a specific user, set the consent level, and designate specific programs for which error reports could be sent. However, centrally restricting the ability to execute PerfTrack to limit the potential for unauthorized or undesired usage, data leakage, or unintentional communications is highly recommended.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Trouble shooting and Diagnostics\Windows Performance PerfTrack\Enable/Disable PerfTrack Impact: If you disable this policy setting, responsiveness events are not processed.

Failed Instances
i-03e085d4f68678768

18.8.43.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider. The recommended state for this setting is: Enabled. Rationale A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client Impact: If you enable this policy setting, you can set the local computer clock to synchronize time with NTP servers.

Failed Instances
i-03e085d4f68678768

18.8.43.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only)

Severity
High

Description
Description This policy setting allows you to specify whether the Windows NTP Server is enabled. The recommended state for this setting is: Disabled. Rationale The configuration of proper time synchronization is critically important in a corporate environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server Impact: If you disable or do not configure this policy setting, your computer cannot service NTP requests from other computers.

Failed Instances
i-03e085d4f68678768

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Severity
High

Description
Description This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices Impact: If you enable this policy setting, AutoPlay is not allowed for MTP devices like cameras or phones.

Failed Instances
i-03e085d4f68678768

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Severity
High

Description
Description This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands. Rationale Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting

with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands: Computer Configuration\Policies \Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun Impact: If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to:a) Completely disable autorun commands, orb) Revert back to pre-Windows Vista behavior of automatically executing the autorun command.

Failed Instances
i-03e085d4f68678768

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Severity
High

Description
Description Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives. Rationale An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: All drives: Computer Configuration\Policies\Administrative Templates \Windows Components\AutoPlay Policies\Turn off Autoplay Impact: Users will have to manually launch setup or installation programs that are provided on removable media.

Failed Instances

i-03e085d4f68678768

18.9.13.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this setting is: Enabled. Rationale This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button Impact: If you enable this policy setting the password reveal button will not be displayed after a user types a password in the password entry text box. If you disable or do not configure this policy setting the password reveal button will be displayed after a user types a password in the password entry text box. The policy applies to all Windows components and applications that use the Windows system controls including Internet Explorer.

Failed Instances
i-03e085d4f68678768

18.9.13.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Severity
High

Description
Description By default, all administrator accounts are displayed when you attempt to elevate a running application. The recommended state for this setting is: Disabled. Rationale Users could see the list of administrator accounts, making it slightly easier for

a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation Impact: If you enable this policy setting, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password. If you disable this policy setting, users will be required to always type in a username and password to elevate.

Failed Instances
i-03e085d4f68678768

18.9.16.1 (L1) Ensure 'Turn off desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets. Gadgets are small applets that display information or utilities on the desktop. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn off desktop gadgets Impact: If you enable this setting, desktop gadgets will be turned off.

Failed Instances
i-03e085d4f68678768

18.9.16.2 (L1) Ensure 'Turn Off user-installed desktop gadgets' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to turn off desktop gadgets that have been installed by the user. The recommended state for this setting is: Enabled. Rationale Allowing gadgets could allow users to install custom gadgets that could be malicious.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop Gadgets\Turn Off user-installed desktop gadgets Impact: If you enable this setting, Windows will not run any user-installed gadgets.

Failed Instances
i-03e085d4f68678768

18.9.22.1 (L1) Ensure 'EMET 5.5' or higher is installed

Severity
High

Description
Description The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Rationale EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows

Recommendation
Install EMET 5.5 or higher.

Failed Instances
i-03e085d4f68678768

18.9.22.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)

Severity
High

Description
Description This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation

Settings - EnabledDeep Hooks - EnabledAnti Detours - EnabledBanned Functions - EnabledExploit Action - User Configured Rationale These advanced mitigations for ROP mitigations apply to all configured software in EMET. Deep Hooks protects critical APIs and the subsequent lower level APIs used by the top level critical API. Anti Detours renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue. Banned Functions will block calls to ntdll!LdrHotPatchRoutine to mitigate potential exploits abusing the API.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to Internet Explorer. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Internet Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if EMET mitigations are applied to other popular software. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled'

Severity
High

Description
Description This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java. The recommended state for this setting is: Enabled. Rationale Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Recommendation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'

Severity
High

Description
Description This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In. Rationale ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-In: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System ASLR Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description

Description This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System DEP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.22.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out'

Severity
High

Description
Description This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP). The recommended state for this setting is: Enabled: Application Opt-Out. Rationale When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System SEHOP Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Failed Instances
i-03e085d4f68678768

18.9.24.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description

Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description

Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 196,608 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances
i-03e085d4f68678768

18.9.24.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrativ e Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they

can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances
i-03e085d4f68678768

18.9.24.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Severity
High

Description
Description This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled. Note: Old events may or may not be retained according to the "Backup log automatically when full"# policy setting. Rationale If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Failed Instances

i-03e085d4f68678768

18.9.24.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Severity
High

Description
Description This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater. Rationale If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Failed Instances

i-03e085d4f68678768

18.9.28.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Severity
High

Description
Description Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled. Rationale Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer Impact: Enabling this policy setting may allow certain legacy plug-in applications to function. Disabling this policy setting will ensure that Data Execution Prevention blocks certain types of malware from exploiting Explorer.

Failed Instances
i-03e085d4f68678768

18.9.28.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Severity
High

Description
Description Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled. Rationale Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off heap termination on corruption Impact:

Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately although Explorer may still terminate unexpectedly later.

Failed Instances
i-03e085d4f68678768

18.9.28.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled. Rationale Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\File Explorer\Turn off shell protocol protected mode Impact: If you enable this policy setting the protocol is fully enabled allowing the opening of folders and files. If you disable this policy setting the protocol is in the protected mode allowing applications to only open a limited set of folders.

Failed Instances
i-03e085d4f68678768

18.9.35.1 (L2) Ensure 'Turn off location' is set to 'Enabled'

Severity
High

Description

Description This policy setting turns off the location feature for this computer. The recommended state for this setting is: Enabled. Rationale This setting affects the location feature (e.g. GPS or other location tracking). From a security perspective, it#x2019;s not a good idea to reveal your location to software in most cases, but there are legitimate uses, such as mapping software.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\Turn off location Impact: If you enable this policy setting, the location feature is turned off, and all programs on this computer are prevented from using location information from the location feature.

Failed Instances
i-03e085d4f68678768

18.9.48.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Severity
High

Description
Description This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server. The recommended state for this setting is: Enabled. Rationale An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Connection Client \Do not allow passwords to be saved Impact: If you enable this policy setting, the password saving checkbox is disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Failed Instances
i-03e085d4f68678768

18.9.48.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to restrict users to a single Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale This setting ensures that users & administrators who Remote Desktop to a server will continue to use the same session - if they disconnect and reconnect, they will go back to the same session they were using before, preventing the creation of a second simultaneous session. This both prevents unnecessary resource usage by having the server host unnecessary additional sessions (which would put extra load on the server) and also ensures a consistency of experience for the user.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections \Restrict Remote Desktop Services users to a single Remote Desktop Services session Impact: If you enable this policy setting, users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.If you disable this policy setting, users are allowed to make unlimited simultaneous remote connections by using Remote Desktop Services.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for COM port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection Impact: If you enable this policy setting, users cannot redirect server data to the local COM port.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient \<driveletter>$ If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled. Rationale Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection Impact: Drive redirection will not be possible. In most cases, traditional network drive mapping to file shares (including

administrative shares) will serve as a capable substitute to still allow file transfers when needed.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session. The recommended state for this setting is: Enabled. Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for LPT port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection Impact: If you enable this policy setting, users in a Remote Desktop Services session cannot redirect server data to the local LPT port.

Failed Instances
i-03e085d4f68678768

18.9.48.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled.

Rationale In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for Plug and Play device redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow supported Plug and Play device redirection Impact: If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client. Note: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent. The recommended state for this setting is: Enabled. Rationale Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection Impact: Users will always have to enter their password when they establish new Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled. Rationale Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication Impact: If you enable this policy setting, the terminal server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Failed Instances
i-03e085d4f68678768

18.9.48.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Severity

High

Description
Description This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. The recommended state for this setting is Enabled: High Level. Rationale If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: High Level: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Security\Set client connection encryption level Impact: Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Failed Instances
i-03e085d4f68678768

18.9.48.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'

Severity
High

Description
Description This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected. The recommended state for this setting is: Enabled: 15 minutes or less. Rationale This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of inactive sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 15 minutes or less: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for active but idle Remote Desktop Services sessions Impact: If you enable this policy setting, you must select the desired time limit in the Idle session limit list. Remote Desktop Services will automatically disconnect active but idle sessions after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply.

Failed Instances
i-03e085d4f68678768

18.9.48.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. The recommended state for this setting is: Enabled: 1 minute. Rationale This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of disconnected but still active sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service. This setting is important to ensure a disconnected session is properly terminated.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Policies\Administrative Templates \Windows Components\Remote Desktop Services\Remote Desktop Session Host \Session Time Limits\Set time limit for disconnected sessions Impact: If you enable

this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled. Rationale Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Do not delete temp folders upon exit Impact: If you disable this policy setting, temporary folders are deleted when a user logs off, even if the server administrator specifies otherwise.

Failed Instances
i-03e085d4f68678768

18.9.48.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Severity
High

Description
Description By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the

temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled. Rationale By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session Impact: If this setting is enabled, only one temporary folder is used for all remote sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Failed Instances
i-03e085d4f68678768

18.9.49.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Severity
High

Description
Description This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled. Rationale Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures Impact: If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.

Failed Instances
i-03e085d4f68678768

18.9.50.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled. Rationale Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: The search service components (including non-Microsoft components) will not encrypted items or encrypted stores.

Failed Instances
i-03e085d4f68678768

18.9.67.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'

Severity
High

Description
Description This setting allows you to set the default consent handling for error reports. The recommended state for this setting is: Enabled: Always ask before sending data Rationale Error reports may contain sensitive information and should not be sent to anyone automatically.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Always ask before sending data: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\Configure Default consent Impact: By setting to always ask before sending data: Windows prompts users for consent to send reports.

Failed Instances
i-03e085d4f68678768

18.9.69.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Severity
High

Description
Description Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled. Rationale In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs Impact: If you

disable or do not configure this policy setting, the security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.

Failed Instances
i-03e085d4f68678768

18.9.69.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Severity
High

Description
Description Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled. Rationale Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs,

this will prevent standard users from installing applications that affect system-wide configuration items.

Failed Instances
i-03e085d4f68678768

18.9.69.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows Web-based programs to install software on the computer without notifying the user. The recommended state for this setting is: Disabled. Rationale Suppressing the system warning can pose a security risk and increase the attack surface on the system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows Installer scripts Impact: If you disable or do not configure this policy setting by default when a script hosted by an Internet browser tries to install a program on the system the system warns users and allows them to select or refuse the installation. If you enable this policy setting the warning is suppressed and allows the installation to proceed. This policy setting is designed for enterprises that use Web-based tools to distribute programs to their employees. However because this policy setting can pose a security risk it should be applied cautiously.

Failed Instances
i-03e085d4f68678768

18.9.79.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'

Severity
High

Description

Description This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for this setting is: Disabled. Rationale Due to the potential risks of capturing passwords in the logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, logging of PowerShell script input is disabled.

Failed Instances
i-03e085d4f68678768

18.9.79.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Severity
High

Description
Description This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled. Rationale If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file.

Recommendation
To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates \Windows Components\Windows PowerShell\Turn on PowerShell Transcription Note: This Group Policy path does not exist by default. A newer version of the "powershelle xecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the Start-Transcript cmdlet.

Failed Instances
i-03e085d4f68678768

18.9.81.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy

setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication. The recommended state for this setting is: Enabled. Rationale Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication Impact: The WinRM client will not use Digest authentication.

Failed Instances
i-03e085d4f68678768

18.9.81.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client. The recommended state for this setting is: Disabled. Rationale Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled. Rationale Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic Impact: None - this is the default behavior.

Failed Instances
i-03e085d4f68678768

18.9.81.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Severity
High

Description
Description This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely. If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset. The recommended state for this setting is: Enabled. Rationale Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If

a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer.If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Failed Instances
i-03e085d4f68678768

18.9.82.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands. The recommended state for this setting is: Disabled. Rationale Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Shell on trusted networks and when feasible employ additional controls such as IPsec.

Recommendation
To implement the recommended configuration state, set the following Group Policy setting to Disabled. Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access Impact: If you disable or do not configure this policy setting, remote access is not allowed to all supported shells to execute scripts and commands.

Failed Instances
i-03e085d4f68678768

18.9.85.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection

is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: Enabled. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Severity
High

Description
Description This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before

downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: 0 - Every day. Rationale Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to 0 - Every day: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

Failed Instances
i-03e085d4f68678768

18.9.85.3 (L1) Ensure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. The recommended state for this setting is: Disabled. Rationale Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Administrative Templates\Windows Components \Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box Impact: If you disable or do not configure this policy

setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.4 (L1) Ensure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' is set to 'Disabled'

Severity
High

Description
Description This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is displayed in the Shut Down Windows dialog box. The recommended state for this setting is: Disabled. Rationale Alerting users that a system needs to be patch is a good way to help ensure patching is being applied to a system.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box Impact: If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be available in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

Failed Instances
i-03e085d4f68678768

18.9.85.5 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Severity
High

Description
Description This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a

scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are:- Enabled- Disabled- Not Configured Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: Disabled. Rationale Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations Impact: If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

Failed Instances
i-03e085d4f68678768

18.9.85.6 (L1) Ensure 'Reschedule Automatic Updates scheduled installations' is set to 'Enabled: 1 minute'

Severity
High

Description
Description This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. The recommended state for this setting is: Enabled: 1 minute. Rationale Rescheduling

automatic updates that were not installed on schedule will help ensure security patches get installed.

Recommendation
To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute: Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations Impact: Remaining Automatic Updates will start 1 minute after the computer restarts.

Failed Instances
i-03e085d4f68678768

4.2: Findings details - Common Vulnerabilities and Exposures-1.1

CVE-2012-2531

Severity
Medium

Description
Microsoft Internet Information Services (IIS) 7.5 uses weak permissions for the Operational log, which allows local users to discover credentials by reading this file, aka "Password Disclosure Vulnerability."

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2531

Failed Instances
i-03e085d4f68678768

CVE-2012-2532

Severity
High

Description

Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability."

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2532

Failed Instances
i-03e085d4f68678768

CVE-2017-5715

Severity
Medium

Description
Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715

Failed Instances
i-03e085d4f68678768

CVE-2017-5753

Severity
Medium

Description
Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753

Failed Instances
i-03e085d4f68678768

CVE-2017-5754

Severity
Medium

Description
Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754

Failed Instances
i-03e085d4f68678768

CVE-2018-0741

Severity
Medium

Description
The Color Management Module (Icm32.dll) in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an information disclosure vulnerability due to the way objects are handled in memory, aka "Microsoft Color Management Information Disclosure Vulnerability".

Recommendation

Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0741

Failed Instances
i-03e085d4f68678768

CVE-2018-0747

Severity
Low

Description
The Windows kernel in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka "Windows Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0745 and CVE-2018-0746.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0747

Failed Instances
i-03e085d4f68678768

CVE-2018-0748

Severity
Medium

Description
The Windows kernel in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way memory addresses are handled, aka "Windows Elevation of Privilege Vulnerability".

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0748

Failed Instances
i-03e085d4f68678768

CVE-2018-0749

Severity
Medium

Description
The Microsoft Server Message Block (SMB) Server in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way SMB Server handles specially crafted files, aka "Windows Elevation of Privilege Vulnerability".

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0749

Failed Instances
i-03e085d4f68678768

CVE-2018-0750

Severity
Medium

Description
The Windows GDI component in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an information disclosure vulnerability due to the way objects are handled in memory, aka "Windows Elevation of Privilege Vulnerability".

Recommendation

Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0750

Failed Instances
i-03e085d4f68678768

CVE-2018-0754

Severity
Medium

Description
The Windows Adobe Type Manager Font Driver (Atmfd.dll) in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are handled in memory, aka "OpenType Font Driver Information Disclosure Vulnerability".

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0754

Failed Instances
i-03e085d4f68678768

CVE-2018-0762

Severity
High

Description
Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique

from CVE-2018-0758, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0762

Failed Instances
i-03e085d4f68678768

CVE-2018-0772

Severity
High

Description
Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0772

Failed Instances
i-03e085d4f68678768

CVE-2018-0788

Severity
High

Description
The Windows Adobe Type Manager Font Driver (Atmfd.dll) in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 and R2 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "OpenType Font Driver Elevation of Privilege Vulnerability".

Recommendation
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0788

Failed Instances
i-03e085d4f68678768

4.3: Findings details - Runtime Behavior Analysis-1.0

Insecure client protocols (general)

Severity
Low

Description
This rule detects client use of insecure protocols.

Recommendation
It is recommended that you replace these insecure protocols with encrypted versions.

Failed Instances
i-03e085d4f68678768

Insecure server protocols

Severity
Informational

Description
This rule helps determine whether your EC2 instances are hosting insecure services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

Recommendation
We recommend you disable insecure protocols in your assessment target and replace them with secure alternatives as listed below: - Disable telnet, rsh, and rlogin and replace them with SSH. Where this is not possible, you should ensure that the insecure service is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups. - Replace FTP with SCP or SFTP where possible. Where this is not possible, you should ensure that the FTP server is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups. - Replace HTTP with HTTPS where possible. For more information specific to the web server in question see http://nginx.org/en/docs/http/configuring_https_servers.html and https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html. - Disable IMAP, POP3, SMTP services if not required. If required, it's recommended these email protocols should be used with encrypted protocols such as TLS. - Disable SNMP service if not required. If required, replace SNMP v1, v2 with more secure SNMP v3 which uses encrypted communication.

Failed Instances
i-03e085d4f68678768

Unused listening TCP ports

Severity
Informational

Description
This rule detects listening TCP ports that may not be required by the assessment target.

Recommendation
To reduce the attack surface area of your deployments, we recommend that you disable network services that you do not use. Where network services are required, we recommend that you employ network control mechanisms such as VPC ACLs, EC2 security groups, and firewalls to limit exposure of that service.

Failed Instances
i-03e085d4f68678768

4.4: Findings details - Security Best Practices-1.0

No findings were generated for this rules package.