ESXi.apply-patches

Keep ESXi system properly patched

Vulnerability Procedure:
By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client select the host and click "Summary". Expand "Configuration" and verify "ESX/ESXi Version" and "Image Profile" strings. Those strings would tell you the current image version of the host. Ensure that the image version is the latest one given by VMware.

Web Client Remediation Procedure:
Employ a process to keep ESXi hosts up to date with patches in accordance with industry-standards and internal guidelines. VMware Update Manager is an automated tool that can greatly assist with this. VMware also publishes Advisories on security patches, and offers a way to subscribe to email alerts for them.
https://www.vmware.com/support/policies/security_response

Desired Value	Default Value	Able to set via Host Profiles
NA	NA	NO

Configuration Parameters	Risk Profile
NA	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli software profile get / # esxcli software vib get	# esxcli software profile update / # esxcli software vib update

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> software profile get / # esxcli <conn_options> software vib get	# esxcli conn_options software profile update / # esxcli conn_options software vib update

PowerCLI Command Assessment	PowerCLI Command Remediation
# VMware Update Manager PowerCLI Cmdlets can be used to check this feature	# VMware Update Manager PowerCLI Cmdlets can be used to check this feature

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.update_manager.doc/GUID-EF6BEE4C-4583-4A8C-81B9-5B074CA2E272.html
https://www.vmware.com/support/policies/security_response

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.PatchManager.Status.html

ESXi.audit-exception-users

Audit the list of users who are on the Exception Users List and whether the have administrator privleges

Vulnerability Procedure:
In vSphere 6.0 and later, you can add users to the Exception Users list from the vSphere Web Client. These users do not lose their permissions when the host enters lockdown mode. Usually you may want to add service accounts such as a backup agent to the Exception Users list. Verify that the list of users who are exempted from losing permissions is legitimate and as needed per your enviornment. Users who do not require special permissions should not be exempted from lockdown mode.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select host and click on "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until "Lockdown Mode". Verify that the list of "Exception Users" is legitimate.

Web Client Remediation Procedure:
From the vSphere web client, select host and click on "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until "Lockdown Mode". Click "Edit" and then click on "Exception Users". Add or delete users as per your site requirements.

Desired Value	Default Value	Able to set via Host Profiles
Site-specific	Null	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation

vCLI Shell Command Assessment	VCLI Shell Command Remediation

PowerCLI Command Assessment	PowerCLI Command Remediation
#Sample code to check each local user on an ESXi host #against the list in vCenter's exception user list. Also checks #to see if the local user has administrator privleges. # # Provide the username and password of an account on your ESXi hosts. # Provide the name of your vCenter Server $esxusername = "root" $esxpassword = "VMware1!" $vCenterServer = "vcsa.lab.local" #Ensure all connections are dropped. Disconnect-VIServer -Force -server * -Confirm:$false # You may need to provide the username and password of your vCenter server below	

```
connect-viserver $vCenterServer
$esxihosts = get-vmhost
#
foreach ($esxihost in $esxihosts)
{
Write-Host "Host is: " $esxihost
Write-host "Exception Users from vCenter"
$myhost = Get-VMHost $esxihost | Get-View
$lockdown = Get-View
$myhost.ConfigManager.HostAccessManager
$LDusers = $lockdown.QueryLockdownExceptions()
Write-host $LDusers
# Connect to each ESXi host in the cluster to retrieve the
list of local users.
Write-Host "Lockdown user: " $LDuser
   Write-host "Connecting to: " $esxihost
   Connect-VIServer -Server $esxihost -user
$esxusername -Password $esxpassword
#Loop through the list of Exception Users and check to
see if they have accounts on
#the ESXi server and if that account in an administrator
account.
foreach ($LDuser in $LDusers)
   {
   Write-host "Get-vmhostaccount"
   $hostaccountname = get-vmhostaccount   -ErrorAction
SilentlyContinue  $LDuser
   write-host "Check to see if user exists"
   if ($hostaccountname.Name)
   Write-Host $hostaccountname.Name
      {
      Write-Host "Get-VIPermission"
      $isadmin = Get-VIPermission -Principal $LDuser -
ErrorAction SilentlyContinue | Where {$_.Role –eq
“Admin”}
      Write-host "Admin Role: " $isadmin.Role
      if ($isadmin.Role -eq "Admin") {Write-Host $LDuser is
an "Exception User with Admin accounts on " $esxihost}
      }
    Disconnect-VIServer -Server $global:DefaultVIServer -
Force  -Confirm:$false

   }
}
```

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-6CD8C2E3-7925-4706-8271-F42F2BCFF95D.html
http://blogs.vmware.com/vsphere/2015/03/vsphere-6-0-lockdown-mode-exception-users.html

vSphere API:

ESXi.config-ntp

Configure NTP time synchronization

Vulnerability Procedure:

By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC), you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.

Negative Functional Impact (if applicable)

None

Web Client Assessment Procedure:

From the vSphere web client select the host and click "Manage" -> "Time Configuration" and click the "Edit..." button. Provide the name/IP of your NTP servers, start the NTP service and change the startup policy to "Start and stop with host". Notes: verify the NTP firewall ports are open. It is recommended to synchronize the ESXi clock with a time server that is located on the management network rather than directly with a time server on a public network. This time server can then synchronize with a public source through a strictly controlled network connection with a firewall.

Web Client Remediation Procedure:

In the vSphere Web Client, select the host in the vCenter inventory. Select Manage -> Settings. In the System Section, select Time Configuration and click Edit. Select "Use Network Time Protocol (Enable NTP client), set the NTP service startup policy, enter the IP addresses of the NTP servers to synchronize with, and click Start or Restart.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	Null	YES

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# vicfg-ntp <conn_options> --list	# vicfg-ntp conn_options --add IP

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the NTP Settings for all hosts Get-VMHost | Select Name, @{N="NTPSetting";E={$_ | Get-VMHostNtpServer}}	# Set the NTP Settings for all hosts $NTPServers = "pool.ntp.org", "pool2.ntp.org"Get- VMHost | Add-VmHostNtpServer $NTPServers

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-2553C86E-7981-4F79-B9FC-A6CECA52F6CC.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.DateTimeSystem.html

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.config-persistent-logs

Configure persistent logging for all ESXi host

Vulnerability Procedure:

ESXi can be configured to store log files on an in-memory file system. This occurs when the host's "/scratch" directory is linked to "/tmp/scratch". When this is done only a single day's worth of logs are stored at any time. In addition log files will be reinitialized upon each reboot. This presents a security risk as user activity logged on the host is only stored temporarily and will not persistent across reboots. This can also complicate auditing and make it harder to monitor events and diagnose issues. ESXi host logging should always be configured to a persistent datastore.

Negative Functional Impact (if applicable)

None

Web Client Assessment Procedure:

From the vSphere web client select the host and click "Manage" -> "Settings" -> "Advanced System settings". Look for "Syslog.global.logDir" parameter name and ensure that it is not set to "[] /scratch/log" or is not blank.

Web Client Remediation Procedure:

1. Identify the datastore path where you want to place scratch, then login to the vSphere Web Client.
2. Navigating to the host and select "Manage" and select "Advanced System Settings" in the System panel.
3. Enter "Syslog.global.LogDir" in the filter. Set the "Syslog.global.LogDir" to the desired datastore path.

Note: the Syslog.global.LogDir must be set for each host.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	[] /scratch/log	YES

Configuration Parameters	Risk Profile
Syslog.global.logDir	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli system syslog config get	# esxcli system syslog config set --logDir

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> system syslog config get	# esxcli conn_options system syslog config set --logDir

PowerCLI Command Assessment	PowerCLI Command Remediation
# List Syslog.global.logDir for each host Get-VMHost | Select Name, @{N="Syslog.global.logDir";E={$_ | Get-VMHostAdvancedConfiguration Syslog.global.logDir | Select -ExpandProperty Values}}	# Set Syslog.global.logDir for each host Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name Syslog.global.logDir -Value "NewLocation" }

Reference Documentation:

http://kb.vmware.com/kb/1033696
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

ESXi.config-snmp

Ensure proper SNMP configuration

Vulnerability Procedure:
If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured. If SNMP is not properly configured, monitoring information can be sent to a malicious host that can then use this information to plan an attack. Note: ESXi 5.1 and later supports SNMPv3 which provides stronger security than SNMPv1 or SNMPv2, including key authentication and encryption.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client select the host and click "Manage" -> "Settings" -> "Security Profile". Look for "SNMP Server" under "Services" section. Its status should be "Stopped" until and unless you are using snmp in your enviornment.

Web Client Remediation Procedure:
You do not configure the SNMP agent with the vSphere Web Client. Use esxcli, PowerCLI, or the vSphere Web Services SDK.

Desired Value	Default Value	Able to set via Host Profiles
site-specific	Disabled	YES

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli system snmp get	# Configure Community String esxcli system snmp set --communities [COMMUNITY] # Configure SNMP Targetesxcli system snmp set --targets [TARGET]@[PORT]/[COMMUNITY] # Enable SNMPesxcli system snmp set --enable true

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> system snmp get	# Configure Community String esxcli conn_options system snmp set --communities [COMMUNITY] # Configure SNMP Target esxcli conn_options system snmp set --targets [TARGET]@[PORT]/[COMMUNITY] # Enable SNMP esxcli conn_options system snmp set --enable true

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the SNMP Configuration of a host (single host connection required) Get-VMHost | Get-VMHostSnmp	# Update the host SNMP Configuration (single host connection required) Get-VmHostSNMP | Set-VMHostSNMP -Enabled:$true -ReadOnlyCommunity 'secret'

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.monitoring.doc/GUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-4309DE28-AFB6-4B2D-A8EA-A38D36A8C6E6.html
SNMP V3 configuration - http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.monitoring.doc/GUID-2E4B0F2A-11D8-4649-AC6C-99F89CE93026.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.SnmpSystem.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.disable-mob

Disable Managed Object Browser (MOB)

Vulnerability Procedure:
The managed object browser (MOB) provides a way to explore the object model used by the VMkernel to manage the host; it enables configurations to be changed as well. This interface is meant to be used primarily for debugging the vSphere SDK. In Sphere 6.0 this is disabled by default

Negative Functional Impact (if applicable)
None. This is disabled by default..

Web Client Assessment Procedure:
Open the Web Client, Select the settings for the host, Select "Advanced System Settings" and search for "Config.HostAgent.plugins.solo.enableMob". Ensure the value is False (default in 6.0 and later).

Web Client Remediation Procedure:
Open the Web Client, Select the settings for the host, Select "Advanced System Settings" and search for "Config.HostAgent.plugins.solo.enableMob" and set the value to False if it isn't currently False.

Desired Value	Default Value	Able to set via Host Profiles
False	false	YES

Configuration Parameters	Risk Profile
Config.HostAgent.plugins.solo.enableMob	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
vim-cmd hostsvc/advopt/view Config.HostAgent.plugins.solo.enableMob	vim-cmd hostsvc/advopt/update Config.HostAgent.plugins.solo.enableMob bool true

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
Get-VMHost <host> | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob	Get-VMHost <host> | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob |Set-AdvancedSetting -value "false"

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-0EF83EA7-277C-400B-B697-04BDC9173EA3.html

vSphere API:
N/A

ESXi.enable-auth-proxy

When adding ESXi hosts to Active Directory use the vSphere Authentication Proxy to protect passwords

Vulnerability Procedure:
If you configure your host to join an Active Directory domain using Host Profiles the Active Directory credentials are saved in the host profile and are transmitted over the network. To avoid having to save Active Directory credentials in the Host Profile and to avoid transmitting Active Directory credentials over the network use the vSphere Authentication Proxy.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
There is no way to audit this using web client if you manually chose to join the host to a domain.
If you chose to join the host to domain by attaching a host profile, you can verify that the host profile has been configured to use proxy server for joining the host to domains by follow below steps:
Go to "Home" and click on "Host Profiles" under "Monitoring" section. Choose the appropriate host profile and expand "Security and Services" -> "Authentication Configuration" -> "Active Directory Configuration". Verify that the "JoinDomain Method" setting is configured to "Use vSphere Authentication Proxy to add the host to Domain".

Web Client Remediation Procedure:
You can do it in two ways - either from Web Client directly or via Host Profiles. For web client, select the host and click on "Manage" -> "Settings" -> "Authentication Services". Click on "Join Domain" and then select "Using Proxy Server" radio button. Provide proxy server IP address.
Using Host profile method,
Install and configure the Authentication proxy. From the vSphere web client, navigate to "Host Profiles", select the host profile, select "Manage" -> "Edit Host profile". Expand "Security and Services" -> "Security Settings" -> "Authentication Configuration". Select "Active Directory configuration". Set the "Join Domain Method" to "Use vSphere Authentication Proxy to add the host do domain" and provide the IP address of the authentication proxy.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	Disabled	YES

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# vicfg-authconfig <conn_options> --authscheme AD --currentdomain	# vicfg-authconfig conn_options ad_conn_options --authscheme AD --joindomain domain_FQDN

PowerCLI Command Assessment	PowerCLI Command Remediation
# Check the host profile is using vSphere Authentication proxy to add the host to the domain Get-VMHost | Select Name, ` @{N="HostProfile";E={$_ \| Get-VMHostProfile}}, ` @{N="JoinADEnabled";E={($_ | Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, ` @{N="JoinDomainMethod";E={(($_ | Get-	# Join the ESXI Host to the Domain Get-VMHost HOST1 | Get-VMHostAuthentication |

VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory | Select -ExpandProperty Policy | Where {$_.Id -eq "JoinDomainMethodPolicy"}).Policyoption.Id}}# Check each host and their domain membership statusGet-VMHost | Get-VMHostAuthentication | Select VmHost, Domain, DomainMembershipStatus	Set-VMHostAuthentication -Domain domain.local -User Administrator -Password Passw0rd -JoinDomain

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-084B74BD-40A5-4A4B-A82C-0C9912D580DC.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.ActiveDirectoryAuthentication.html

ESXi.enable-chap-auth

Enable bidirectional CHAP, also known as Mutual CHAP, authentication for iSCSI traffic

Vulnerability Procedure:
vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. Choosing not to enforce more stringent authentication can make sense if you create a dedicated network or VLAN to service all your iSCSI devices. By not authenticating both the iSCSI target and host, there is a potential for a MiTM attack in which an attacker might impersonate either side of the connection to steal data. Bidirectional authentication can mitigate this risk. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select a host and click on "Manage" -> "Storage" -> "Storage Adapters".
For EACH iSCSI Adapter, scroll for "Authentication" section under "Adapter Details" section -> "Properties" tab. The "Method" parameter should be set to "Use bidirectional CHAP".

Web Client Remediation Procedure:
From the vSphere web client, select a host and click on "Manage" -> "Storage" -> "Storage Adapters".
For EACH iSCSI Adapter, scroll for "Authentication" section under "Adapter Details" section -> "Properties" tab. Click "Edit" and configure bidirectional chap authentication.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	No Authentication	NO

Configuration Parameters	Risk Profile
Use Chap, Name, Secret	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli iscsi adapter auth chap get	# esxcli iscsi adapter auth chap set

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> iscsi adapter auth chap get	# esxcli iscsi conn_options adapter auth chap set

PowerCLI Command Assessment	PowerCLI Command Remediation
# List Iscsi Initiator and CHAP Name if defined Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} \| Select VMHost, Device, ChapType, @{N="CHAPName";E={$_.AuthenticationProperties.ChapName}}	# Set the Chap settings for the Iscsi Adapter Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use desired parameters here

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-DFC745FB-CDD6-4828-8948-4D0E0561EEF8.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.InternetScsiHba.AuthenticationProperties.html

ESXi.enable-normal-lockdown-mode

Enable Normal Lockdown Mode to restrict access

Vulnerability Procedure:

Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server. This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging into a host directly. By forcing all interaction to occur through vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced. Note: Lockdown mode does not apply to users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH even when the host is in lockdown mode.
Note that users listed in the DCUI.Access list for each host are allowed to override lockdown mode and login to the DCUI.
By default the "root" user is the only user listed in the DCUI.Access list.

Negative Functional Impact (if applicable)

There are some operations, such as backup and troubleshooting, that require direct access to the host. In these cases Lockdown Mode can be disabled on a temporary basis for specific hosts as needed, and then re-enabled when the task is completed.
Note: L

Web Client Assessment Procedure:

From the vSphere web client, select host and click on "Manage" -> "Settings" -> "System" -> "Security Profile".
Scroll down until "Lockdown Mode". Verify that "Lockdown Mode" parameter is set to "Enabled (Normal)".

Web Client Remediation Procedure:

From the vSphere web client, select host and click on "Manage" -> "Settings" -> "System" -> "Security Profile".
Scroll down until "Lockdown Mode". Click "Edit" and then choose "Normal".

Desired Value	Default Value	Able to set via Host Profiles
Enabled	Disabled	YES

Configuration Parameters	Risk Profile
vimsvc/auth/lockdown_is_enabled	2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# To check if Lockdown mode is enabled: #Note: This will not differentiate between Normal and Strict. #If either are enabled the result will be "true" vim-cmd -U dcui vimsvc/auth/lockdown_is_enabled	# To disable Lockdown mode: vim-cmd -U dcui vimsvc/auth/lockdown_mode_exit #Enabling strict lockdown mode is not supported by vim-cmd. # To enable Normal Lockdown mode: vim-cmd -U dcui vimsvc/auth/lockdown_mode_enter

vCLI Shell Command Assessment	VCLI Shell Command Remediation

PowerCLI Command Assessment	PowerCLI Command Remediation
# To check if Lockdown mode is enabled Get-VMHost | Select Name,@{N="Lockdown";E={$_.Extensiondata.Config.adminDisabled}}	# Enable lockdown mode for each host Get-VMHost | Foreach { $_.EnterLockdownMode() }

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html
http://kb.vmware.com/kb/1008077

vSphere API:
http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.HostSystem.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.enable-remote-syslog

Configure remote logging for ESXi hosts

Vulnerability Procedure:
Remote logging to a central log host provides a secure, centralized store for ESXi logs. By gathering host log files onto a central host you can more easily monitor all hosts with a single tool. You can also do aggregate analysis and searching to look for such things as coordinated attacks on multiple hosts. Logging to a secure, centralized log server helps prevent log tampering and also provides a long-term audit record. To facilitate remote logging VMware provides the vSphere Syslog Collector.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere Web Client select the host, click "Manage" -> "Advanced Sytem Settings", and enter "Syslog.global.logHost" in the filter. Check whether a syslog host is set.

Web Client Remediation Procedure:
Step 1: Install/Enable a syslog host (vSphere Syslog Collector recommended).
Step 2: From the vSphere Web Client select the host and click "Manage" -> "Advanced Sytem Settings", and enter "Syslog.global.logHost" in the filter. Set the "Syslog.global.logHost" to the hostname of your syslog server.
Note: when setting a remote log host it is also recommended to set the "Syslog.global.logDirUnique" to true. You must configure the syslog settings for each host. The host syslog parameters can also be configured the vCLI or PowerCLI, or using an API client.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	No Remote Syslog Host is set	YES

Configuration Parameters	Risk Profile
Syslog.global.logHost	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli system syslog config get	# esxcli system syslog config set loghost # esxcli system syslog reload

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> system syslog config get	# esxcli conn_options system syslog config set loghost # esxcli system syslog reload

PowerCLI Command Assessment	PowerCLI Command Remediation
# List Syslog.global.logHost for each host Get-VMHost | Select Name, @{N="Syslog.global.logHost";E={$_ | Get-VMHostAdvancedConfiguration Syslog.global.logHost | Select -ExpandProperty Values}}	# Set Syslog.global.logHost for each host Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name Syslog.global.logHost -Value "NewLocation" }

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-61E7E2EA-F531-4665-9225-58BA899F55A5.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.enable-strict-lockdown-mode

Enable Strict lockdown mode to restrict access

Vulnerability Procedure:

Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server.
This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging into a host directly. By forcing all interaction to occur through vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced.
Strict lockdown mode stops the DCUI service. However, the ESXi Shell and SSH services are independent of lockdown mode. For lockdown mode to be an effective security measure, ensure that the ESXi Shell and SSH services are also disabled. Those services are disabled by default.
When a host is in lockdown mode, users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host and if these services are enabled. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option.

Negative Functional Impact (if applicable)

In strict lockdown mode, which is new in vSphere 6.0, the DCUI service is stopped. If the connection to vCenter Server is lost and the vSphere Web Client is no longer available, the ESXi host becomes unavailable unless the ESXi Shell and SSH services are

Web Client Assessment Procedure:

From the vSphere Web Client, select the host and click on "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down to "Lockdown Mode". Verify that "Lockdown Mode" parameter is set to "Enabled (Strict)".

Web Client Remediation Procedure:

From the vSphere web client, select host and click on "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down to "Lockdown Mode". Click "Edit" and then choose "Strict".

Desired Value	Default Value	Able to set via Host Profiles
Enabled	Disabled	N/A

Configuration Parameters	Risk Profile
vimsvc/auth/lockdown_is_enabled	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# To check if Lockdown mode is enabled: #Note: This will not differentiate between Normal and Strict. #If either are enabled the result will be "true" vim-cmd -U dcui vimsvc/auth/lockdown_is_enabled	# To disable Lockdown mode: vim-cmd -U dcui vimsvc/auth/lockdown_mode_exit #Enabling strict lockdown mode is not supported by vim-cmd. # To enable Normal Lockdown mode: vim-cmd -U dcui vimsvc/auth/lockdown_mode_enter

vCLI Shell Command Assessment	VCLI Shell Command Remediation

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

PowerCLI Command Assessment	PowerCLI Command Remediation

# To check if Lockdown mode is enabled 	
Get-VMHost | Select
Name,@{N="Lockdown";E={$_.Extensiondata.Config.admin
Disabled}}
#To display the mode
$esxihosts = get-vmhost
foreach ($esxihost in $esxihosts)
{
$myhost = Get-VMHost $esxihost | Get-View
$lockdown = Get-View
$myhost.ConfigManager.HostAccessManager
Write-Host "————————————"
$lockdown.UpdateViewData()
$lockdownstatus = $lockdown.LockdownMode
Write-Host "Lockdown mode on $esxihost is set to
$lockdownstatus"
Write-Host "————————————"
}
	#Run this at the vCenter level or against an individual
	host
	#Create HostLockdownMode object
	$level = New-Object
	VMware.Vim.HostLockdownMode
	#Populate with level of
	lockdown:(lockdownDisabled,lockdownNormal,lockdo
	wnStrict)
	$level = "lockdownStrict"
	$esxih

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html

vSphere API:

http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.HostSystem.html

ESXi.firewall-enabled

Configure the ESXi host firewall to restrict access to services running on the host

Vulnerability Procedure:
Unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to only allow access from authorized networks.

Negative Functional Impact (if applicable)
Only systems in the IP whitelist/ACL will be able to connect to services on the ESXi server

Web Client Assessment Procedure:
From the vSphere web client, select the host and click "Manage" -> "Settings" -> "System" -> "Security Profile".
Verify that for enabled services, both incoming and outgoing connections, a proper network/IP Range is selected (the 3rd column should not be "All").

Web Client Remediation Procedure:
From the vSphere web client, select the host and click "Manage" -> "Settings" -> "System" -> "Security Profile".
For each enabled services for both incoming and outgoing connections set a proper network/IP Range after deselecting "Allow connections from any IP address" checkbox.

Desired Value	Default Value	Able to set via Host Profiles
Site Specific	Connections are allowed from any IP address	YES

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
#List all services: ls /etc/init.d #get service status: /etc/init.d/[SERVICE] status	# /etc/init.d/[SERVICE] STOP

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all services for a host Get-VMHost HOST1 | Get-VMHostService # List the services which are enabled and have rules defined for specific IP ranges to access the service Get-VMHost HOST1 | Get-VMHostFirewallException | Where {$_.Enabled -and (-not $_.ExtensionData.AllowedHosts.AllIP)} # List the services which are enabled and do not have rules defined for specific IP ranges to access the service Get-VMHost HOST1 \| Get-VMHostFirewallException \| Where {$_.Enabled -and ($_.ExtensionData.AllowedHosts.AllIP)}	N/A

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-8912DD42-C6EA-4299-9B10-5F3AEA52C605.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.ServiceSystem.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.set-dcui-access

Set DCUI.Access to allow trusted users to override lockdown mode

Vulnerability Procedure:
Lockdown mode disables direct host access requiring that admins manage hosts from vCenter Server. However, if a host becomes isolated from vCenter Server, the admin is locked out and can no longer manage the host. If you are using normal lockdown mode, you can avoid becoming locked out of an ESXi host that is running in lockdown mode, by setting DCUI.Access to a list of highly trusted users who can override lockdown mode and access the DCUI. The DCUI is not running in strict lockdown mode.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere Web Client select the host, click "Manage" -> "Settings" -> "System" -> "Advanced Sytem Settings". Enter "DCUI.Access" in the filter. Verify that the list of users is legitimate. It should ideally contain root and any other local users who are authorized to override lockdown mode.

Web Client Remediation Procedure:
From the vSphere Web Client select the host, click "Manage" -> "Settings" -> "System" -> "Advanced Sytem Settings". Enter "DCUI.Access" in the filter. Enter comma separated user accounts who are authorized to access DCUI even in case of lockdown mode.
Caution: Do not remove root user.

Desired Value	Default Value	Able to set via Host Profiles
List of authorized users	root	YES

Configuration Parameters	Risk Profile
DCUI.Access	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
vim-cmd hostsvc/advopt/view DCUI.Access	vim-cmd hostsvc/advopt/update DCUI.Access string [USERS]

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-6779F098-48FE-4E22-B116-A8353D19FF56.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

ESXi.set-password-policies

Establish a password policy for password complexity

Vulnerability Procedure:
ESXi uses the pam_passwdqc.so plug-in to set password strength and complexity. It is important to use passwords that are not easily guessed and that are difficult for password generators to determine. Password strength and complexity rules apply to all ESXi users, including root. They do not apply to Active Directory users when the ESX host is joined to a domain. Those password policies are enforced by AD.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Security.PasswordQualityControl to see the configured value. It should be set as default value or more restrictive.

Web Client Remediation Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Security.PasswordQualityControl to see the configured value. Set it to the default value or more restrictive.

Desired Value	Default Value	Able to set via Host Profiles
Site specific	"retry=3 min=disabled,disabled,disabled,7,7"	NO

Configuration Parameters	Risk Profile
Security.PasswordQualityControl	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List Security.PasswordQualityControl for each host Get-VMHost | Select Name, @{N="Security.PasswordQualityControl";E={$_ | Get-VMHostAdvancedConfiguration Security.PasswordQualityControl | Select -ExpandProperty Values}}	# Set Security.PasswordQualityControl for each host #these values are an example. Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name Security.PasswordQualityControl -Value "retry=3 min=8,8,8,7,6" }

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43.html

vSphere API:
N/A

ESXi.set-shell-interactive-timeout

Set a timeout to automatically terminate idle ESXi Shell and SSH sessions

Vulnerability Procedure:
If a user forgets to log out of their SSH session, the idle connection will remains open indefinitely, increasing the potential for someone to gain privileged access to the host. The ESXiShellInteractiveTimeOut allows you to automatically terminate idle shell sessions.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for UserVars.ESXiShellInteractiveTimeOut to see the configured value. It should be set to desired value or more restrictive.

Web Client Remediation Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for UserVars.ESXiShellInteractiveTimeOut to see the configured value. Click edit and set it to the desired value or more restrictive.

Desired Value	Default Value	Able to set via Host Profiles
900	0	NO

Configuration Parameters	Risk Profile
UserVars.ESXiShellInteractiveTimeOut	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellInteractiveTimeOut	# esxcli system settings advanced set -o /UserVars/ESXiShellInteractiveTimeOut -i

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellInteractiveTimeOut	# esxcli conn_options system settings advanced set -o /UserVars/ESXiShellInteractiveTimeOut -i

PowerCLI Command Assessment	PowerCLI Command Remediation
# List UserVars.ESXiShellInteractiveTimeOut for each host Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-VMHostAdvancedConfiguration UserVars.ESXiShellInteractiveTimeOut | Select -ExpandProperty Values}}	# Set UserVars.ESXiShellInteractiveTimeOut to 900 on all hosts Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name UserVars.ESXiShellInteractiveTimeOut -Value 900 }

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-94F0C54F-05E3-4E16-8027-0280B9ED1009.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

http://kb.vmware.com/kb/2004746

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

ESXi.set-shell-timeout

Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run

Vulnerability Procedure:
When the ESXi Shell or SSH services are enabled on a host they will run indefinitely. To avoid having these services left running set the ESXiShellTimeOut. The ESXiShellTimeOut defines a window of time after which the ESXi Shell and SSH services will automatically be terminated.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for UserVars.ESXiShellTimeOut to see the configured value. It should be set to desired value or more restrictive.

Web Client Remediation Procedure:
From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for UserVars.ESXiShellTimeOut to see the configured value. Click edit and set it to the desired value or more restrictive.

Desired Value	Default Value	Able to set via Host Profiles
900	0	NO

Configuration Parameters	Risk Profile
UserVars.ESXiShellTimeOut	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut	# esxcli system settings advanced set -o /UserVars/ESXiShellTimeOut -i

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut	# esxcli conn_options system settings advanced set -o /UserVars/ESXiShellTimeOut -i

PowerCLI Command Assessment	PowerCLI Command Remediation
# List UserVars.ESXiShellTimeOut for each host Get-VMHost | Select Name, @{N="UserVars.ESXiShellTimeOut";E={$_ | Get-VMHostAdvancedConfiguration UserVars.ESXiShellTimeOut | Select -ExpandProperty Values}}	# Set Remove UserVars.ESXiShellTimeOut to 900 on all hosts Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name UserVars.ESXiShellTimeOut -Value 900 }

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-94F0C54F-05E3-4E16-8027-0280B9ED1009.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-B314F79B-2BDD-4D68-8096-F009B87ACB33.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

http://kb.vmware.com/kb/2004746

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

ESXi.TransparentPageSharing-intra-enabled

Ensure default setting for intra-VM TPS is correct

Vulnerability Procedure:

Acknowledgement of the recent academic research that leverages Transparent Page Sharing (TPS) to gain unauthorized access to data under certain highly controlled conditions and documents VMware's precautionary measure of restricting TPS to individual virtual machines by default in upcoming ESXi releases. At this time, VMware believes that the published information disclosure due to TPS between virtual machines is impractical in a real world deployment.
VMs that do not have the sched.mem.pshare.salt option set cannot share memory with any other VMs.

Negative Functional Impact (if applicable)

Web Client Assessment Procedure:

From the vSphere Web Client, select a host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Mem.ShareForceSalting. Verify that it is set to 2.

Web Client Remediation Procedure:

From vSphere Web Client, select a host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Mem.ShareForceSalting. Click edit and set it to 2.

Desired Value	Default Value	Able to set via Host Profiles
2	2	YES

Configuration Parameters	Risk Profile
Mem.ShareForceSalting	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation

vCLI Shell Command Assessment	VCLI Shell Command Remediation

PowerCLI Command Assessment	PowerCLI Command Remediation

$VMHosts = Get-VMHost \| Where {$_.ConnectionState -eq "Connected"}
foreach ($VMHost in $VMHosts) {
Get-VMHostAdvancedConfiguration -VMHost $VMHost -Name "Mem.ShareForceSalting"
}
	$tps = "2"
	$VMHosts = Get-VMHost \| Where {$_.ConnectionState -eq "Connected"}
	foreach ($VMHost in $VMHosts) {
	Set-VMHostAdvancedConfiguration -VMHost $VMHost -Name "Mem.ShareForceSalting" -Value $tps
	}

Reference Documentation:

https://kb.vmware.com/kb/2080735
https://kb.vmware.com/kb/2097593
https://kb.vmware.com/kb/2091682

vSphere API:

ESXi.verify-acceptance-level-accepted

Verify Image Profile and VIB Acceptance Levels

Vulnerability Procedure:

Verify the ESXi Image Profile to only allow signed VIBs. An unsigned VIB represents untested code installed on an ESXi host. The ESXi Image profile supports four acceptance levels:
(1) VMwareCertified - VIBs created, tested and signed by VMware
(2) VMwareAccepted - VIBs created by a VMware partner but tested and signed by VMware
(3) PartnerSupported - VIBs created, tested and signed by a certified VMware partner
(4) CommunitySupported - VIBs that have not been tested by VMware or a VMware partner. Community Supported VIBs are not supported and do not have a digital signature. To protect the security and integrity of your ESXi hosts do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts.

Negative Functional Impact (if applicable)

Third party VIBs tested by VMware partners are not allowed on the host. This could include some device drivers, CIM modules, and other add-on software. Host customization using custom VIBs is not allowed.

Web Client Assessment Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Verify that the "Acceptance Level" parameter is set to "VMware Accepted" or "VMware Certified".

Web Client Remediation Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Click "Edit" and set the "Acceptance Level" parameter to "VMware Accepted".

Desired Value	Default Value	Able to set via Host Profiles
VMware Certified or VMware Accepted	Partner Supported	NO

Configuration Parameters	Risk Profile
N/A	2

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $VMHost \| Select Name, @{N="AcceptanceLevel";E={$ESXCli.software.acceptance.get()}}} # List only the vibs which are not at "VMwareCertified" or "VMwareAccepted" acceptance level Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.vib.list() | Where {	# Set the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.acceptance.Set("VMwareCertified")}

($_.AcceptanceLevel -ne "VMwareCertified") -and ($_.AcceptanceLevel -ne "VMwareAccepted") }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-56600593-EC2E-4125-B1A0-065BDD16CF2D.html

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-751034F3-5337-4DB2-8272-8DAC0980EACA.html

vSphere API:

http://pubs.vmware.com/vsphere60/topic/com.vmware.wssdk.apiref.doc/vim.host.ImageConfigManager.html

ESXi.verify-acceptance-level-certified

Verify Image Profile and VIB Acceptance Levels

Vulnerability Procedure:

Verify the ESXi Image Profile to only allow signed VIBs. An unsigned VIB represents untested code installed on an ESXi host. The ESXi Image profile supports four acceptance levels:
(1) VMwareCertified - VIBs created, tested and signed by VMware
(2) VMwareAccepted - VIBs created by a VMware partner but tested and signed by VMware
(3) PartnerSupported - VIBs created, tested and signed by a certified VMware partner
(4) CommunitySupported - VIBs that have not been tested by VMware or a VMware partner. Community Supported VIBs are not supported and do not have a digital signature. To protect the security and integrity of your ESXi hosts do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts.

Negative Functional Impact (if applicable)

No VMware partner VIBs are allowed on the host, to include non-VMware written device drivers, CIM modules, and other third party software. Host customization using custom VIBs is not allowed.

Web Client Assessment Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Verify that the "Acceptance Level" parameter is set to "VMware Certified".

Web Client Remediation Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Click "Edit" and set the "Acceptance Level" parameter to "VMware Certified".

Desired Value	Default Value	Able to set via Host Profiles
VMware Certified	Partner Supported	NO

Configuration Parameters	Risk Profile
N/A	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $VMHost \| Select Name, @{N="AcceptanceLevel";E={$ESXCli.software.acceptance.get()}}} # List only the vibs which are not at "VMwareCertified" acceptance level	# Set the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.acceptance.Set("VMwareCertified")}

Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.vib.list() | Where { $_.AcceptanceLevel -ne "VMwareCertified" }}	

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-56600593-EC2E-4125-B1A0-065BDD16CF2D.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-751034F3-5337-4DB2-8272-8DAC0980EACA.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.ImageConfigManager.html

ESXi.verify-acceptance-level-supported

Verify Image Profile and VIB Acceptance Levels

Vulnerability Procedure:

Verify the ESXi Image Profile to only allow signed VIBs. An unsigned VIB represents untested code installed on an ESXi host. The ESXi Image profile supports four acceptance levels:
(1) VMwareCertified - VIBs created, tested and signed by VMware
(2) VMwareAccepted - VIBs created by a VMware partner but tested and signed by VMware,
(3) PartnerSupported - VIBs created, tested and signed by a certified VMware partner
(4) CommunitySupported - VIBs that have not been tested by VMware or a VMware partner. Community Supported VIBs are not supported and do not have a digital signature. To protect the security and integrity of your ESXi hosts do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts.

Negative Functional Impact (if applicable)

Host customization using custom VIBs is not allowed.

Web Client Assessment Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Verify that the "Acceptance Level" parameter is set to "VMware Accepted", "VMware Certified" or "Partner Supported".

Web Client Remediation Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Security Profile". Scroll down until you see "Host Image Profile Acceptance Level". Click "Edit" and set the "Acceptance Level" parameter to "Partner Supported".

Desired Value	Default Value	Able to set via Host Profiles
VMware Certified, VMware Accepted or Partner Supported	Partner Supported	NO

Configuration Parameters	Risk Profile
N/A	3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> software acceptance get # esxcli software vib list	# esxcli conn_options software acceptance set --level

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $VMHost \| Select Name, @{N="AcceptanceLevel";E={$ESXCli.software.acceptance.get()}}} # List only the vibs which are not at "VMwareCertified" or "VMwareAccepted" or "PartnerSupported" acceptance level Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.vib.list() \| Where { ($_.AcceptanceLevel -ne "VMwareCertified") -and	# Set the Software AcceptanceLevel for each host Foreach ($VMHost in Get-VMHost) { $ESXCli = Get-EsxCli -VMHost $VMHost $ESXCli.software.acceptance.Set("VMwareCertified")}

($_.AcceptanceLevel -ne "VMwareAccepted") -and ($_.AcceptanceLevel -ne "PartnerSupported") }}	

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-56600593-EC2E-4125-B1A0-065BDD16CF2D.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-751034F3-5337-4DB2-8272-8DAC0980EACA.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.ImageConfigManager.html

SSO.verify-SSO-Lockout-policy

Ensure SSO Lockout policy conforms to local policy

Vulnerability Procedure:
SSO comes with a default strict lockout policy requirements. Ideally, these lockout policy requirements provide a strong security baseline and need not be modified until and unless your site-specific lockout requirement policy is more restrictive.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
Login as SSO administrator on vSphere web client. Expand "Administration" -> "Single Sign-on" and click on "Configuration" -> "Policies" -> "Lockout Policy". Verify that the lockout policy is set as below (default):
Maximum number of failed login attempts - 5
Time interval between failures - 180 seconds
Unlock time - 300 seconds

Web Client Remediation Procedure:
Login as SSO administrator on vSphere web client. Expand "Administration" -> "Single Sign-on" and click on "Configuration" -> "Policies" -> "Lockout Policy". Click "Edit" and configure the lockout policy as per your site-specific requirements.

Desired Value	Default Value	Able to set via Host Profiles
Site-specific	N/A	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-2D25D311-AB56-40F4-9834-BC19A7D2EA3D.html

vSphere API:
N/A

SSO.verify-SSO-Password-policy

Ensure SSO Password policy conforms to local policy

Vulnerability Procedure:
SSO comes with a default strict password policy requirements. Ideally, these password requirements are good enough and need not be modified until and unless your site-specific password requirement policy is more restrictive.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
Login as SSO administrator on vSphere web client. Expand "Administration" -> "Single Sign-on" and click on "Configuration" -> "Policies" -> "Password Policy". Verify that the password policy is set as below (default):
Maximum lifetime - Password must be changed every 90 days
Restrict reuse - Users cannot reuse any previous 5 passwords
Maximum length - 20 characters
Minimum length - 8 characters
Character requirements -
At least 2 alphabetic characters
At least 1 special characters
At least 1 uppercase characters
At least 1 lowercase characters
At least 1 numeric characters
Identical adjacent characters:3

Web Client Remediation Procedure:
Login as SSO administrator on vSphere web client. Expand "Administration" -> "Single Sign-on" and click on "Configuration" -> "Policies" -> "Password Policy". Click "Edit" and configure the password policy as per your site-specific requirements.

Desired Value	Default Value	Able to set via Host Profiles
Site-specific	N/A	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-B9C4409A-B053-40C3-96DE-232BB99AAA35.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vSphere API:
N/A

vCenter.verify-nfc-ssl

Enable SSL for Network File copy (NFC)

Vulnerability Procedure:

NFC (Network File Copy) is the name of the mechanism used to migrate or clone a VM between two ESXi hosts over the network.
By default, NFC over SSL is enabled (ie: "True") within a vSphere cluster but the value of the setting is null.
Clients check the value of the setting and default to not using SSL for performance reasons if the value is null. This behavior can be changed by ensuring the setting has been explicitly created and set to "True". This will force clients to use SSL.

Negative Functional Impact (if applicable)

Using SSL may reduce performance of actions involving NFC, such as VM clone or migration.

Web Client Assessment Procedure:

In the vSphere Web Client, open the Advanced Settings of your vCenter server. Check if the "config.nfc.useSSL" key exists and if so verify that it is set to "true". Even though the default is true, auditing scripts can determine this setting only if the key is set explicitly. Additionally, this will force clients to use SSL.

Web Client Remediation Procedure:

In the vSphere Web Client, open the Advanced Settings of your vCenter server and set "config.nfc.useSSL" to true. If the key does not exists, add it to Advanced Settings. Setting the key explicitly allows auditing scripts to determine the settings. Additionally, this will force clients to use SSL.

Desired Value	Default Value	Able to set via Host Profiles
True	Null	NO

Configuration Parameters	Risk Profile
config.nfc.useSSL	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# Check Network File Copy NFC uses SSL. OS Administrator Privileges will be needed on your server for this to complete $vCenter = "MyvCenterFQDN" $nfcset = get-advancedsetting -entity $vCenter -name config.nfc.useSSL $Write-host $nfcset	$vCenter = "MyvCenterFQDN" $nfcset = get-advancedsetting -entity $vCenter -name config.nfc.useSSL \| set-AdvancedSetting -value true -confirm:$false

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-B58A5750-A15C-4051-BD87-49F3B5C762B5.html

vSphere API:

VM.disable-console-copy

Explicitly disable copy/paste operations

Vulnerability Procedure:
Copy and paste operations are disabled by default. However, if you explicitly disable this feature audit controls can check that this setting is correct.

Negative Functional Impact (if applicable)
This is the default setting so functionality remains the same

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.copy.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.copy.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.copy.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.copy.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.copy.disable" -value $true

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-367D02C1-B71F-4AC3-AA05-85033136A667.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-console-drag-n-drop

Explicitly disable copy/paste operations

Vulnerability Procedure:
Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.
The default value is null. Setting this to true is just for audit.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
True	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.dnd.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i isolation.tools.dnd.disable [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.dnd.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.dnd.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.dnd.disable" -value $true

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-367D02C1-B71F-4AC3-AA05-85033136A667.html

vSphere API:
http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-console-gui-options

Explicitly disable copy/paste operations

Vulnerability Procedure:
Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
FALSE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.setGUIOptions.enable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i isolation.tools.setGUIOptions.enable [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.setGUIOptions.enable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.setGUIOptions.enable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.setGUIOptions.enable" -value $false

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-console-paste

Explicitly disable copy/paste operations

Vulnerability Procedure:
Copy and paste operations are disabled by default, however, if you explicitly disable this feature, audit controls can check that this setting is correct.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.paste.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i isolation.tools.paste.disable [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.paste.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.paste.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.paste.disable" -value $true

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-367D02C1-B71F-4AC3-AA05-85033136A667.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-disk-shrinking-shrink

Disable virtual disk shrinking

Vulnerability Procedure:

Shrinking a virtual disk reclaims unused space in it. The shrinking process itself, which takes place on the host, reduces the size of the disk's files by the amount of disk space reclaimed in the wipe process. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. A non-root user cannot wipe the parts of the virtual disk that require root-level permissions. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature. Repeated disk shrinking can make a virtual disk unavailable. Limited capability is available to non-administrative users in the guest.

Negative Functional Impact (if applicable)

Inability to shrink virtual machine disks in the event that a datastore runs out of space.

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.diskShrink.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.diskShrink.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.diskWiper.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.diskShrink.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.diskShrink.disable" -value $true

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-9610FE65-3A78-4982-8C28-5B34FEB264B6.html

vSphere API:
http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-disk-shrinking-wiper

Disable virtual disk shrinking

Vulnerability Procedure:

Shrinking a virtual disk reclaims unused space in it. VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. Wiping takes place in the guest operating system. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. A non-root user cannot wipe the parts of the virtual disk that require root-level permissions. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature. Repeated disk shrinking can make a virtual disk unavailable. Limited capability is available to non-administrative users in the guest.

Negative Functional Impact (if applicable)

Inability to shrink virtual machine disks in the event that a datastore runs out of space.

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.diskWiper.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.diskWiper.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.diskWiper.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.diskWiper.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.diskWiper.disable" -value $true

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-9610FE65-3A78-4982-8C28-5B34FEB264B6.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-hgfs

Disable HGFS file transfers

Vulnerability Procedure:
Certain automated operations such as automated tools upgrades use a component in the hypervisor called "Host Guest File System" and an attacker could potentially use this to transfer files inside the guest OS

Negative Functional Impact (if applicable)
This will cause the VMX process to not respond to commands from the tools process, this may have a negative impact on operations such as automated tools upgrades

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.hgfsServerSet.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.hgfsServerSet.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.hgfsServerSet.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.hgfsServerSet.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.hgfsServerSet.disable" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-76EF6146-FA0E-467F-826F-C953815218C5.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-independent-nonpersistent

Avoid using independent nonpersistent disks

Vulnerability Procedure:

The security issue with nonpersistent disk mode is that successful attackers, with a simple shutdown or reboot, might undo or remove any traces that they were ever on the machine. To safeguard against this risk, production virtual machines should be set to use persistent disk mode; additionally, make sure that activity within the VM is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector. Without a persistent record of activity on a VM, administrators might never know whether they have been attacked or hacked.

Negative Functional Impact (if applicable)

Won't be able to make use of nonpersistent mode, which allows rollback to a known state when rebooting the VM.

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
One of the following: * Not present (defaults to Persistent if blank) * Explicitly set to Persistent *Set to Independent-Persistent	Persistent	N/A

Configuration Parameters	Risk Profile
scsiX:Y.mode	1,2

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "^scsi[0-9]*:[0-9]*.mode" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
1. vifs --server [SERVER] --username [USERNAME] --password [PASSWORD] -g "[DATASTORE] VM/VM.vmx" VM.vmx 2. grep -i "^scsi[0-9]*:[0-9]*.mode" [VMX]	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
#List the VM's and their disk types Get-VM | Get-HardDisk | Select Parent, Name, Filename, DiskType, Persistence	#Alter the parameters for the following cmdlet to set the VM Disk Type: Get-VM | Get-HardDisk | Set-HardDisk

Reference Documentation:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-1E583D6D-77C7-402E-9907-80B7F478D3FC.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-autologon

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on both vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.ghi.autologon.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.ghi.autologon.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.ghi.autologon.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-unexposed-features-biosbbs

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.bios.bbs.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.bios.bbs.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.bios.bbs.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.bios.bbs.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.bios.bbs.disable" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-unexposed-features-getcreds

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.getCreds.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.getCreds.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.getCreds.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.getCreds.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.getCreds.disable" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-unexposed-features-launchmenu

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.ghi.launchmenu.change	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.ghi.launchmenu.change" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.ghi.launchmenu.change	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-memsfss

Disable certain unexposed features

Vulnerability Procedure:
Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.memSchedFakeSampleStats.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.memSchedFakeSampleStats.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.memSchedFakeSampleStats.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable" -value $true

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-protocolhandler

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.ghi.protocolhandler.info.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.ghi.protocolhandler.info.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.ghi.protocolhandler.info.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-shellaction

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.ghi.host.shellAction.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.ghi.host.shellAction.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.ghi.host.shellAction.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-toporequest

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.dispTopoRequest.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.dispTopoRequest.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.dispTopoRequest.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.disable-unexposed-features-trashfolderstate

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.trashFolderState.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.trashFolderState.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.trashFolderState.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.trashFolderState.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.trashFolderState.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-trayicon

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.ghi.trayicon.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.ghi.trayicon.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.ghi.trayicon.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unity

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unity.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unity.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unity.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unity-interlock

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unityInterlockOperation.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unityInterlockOperation.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unityInterlockOperation.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unitypush

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unity.push.update.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unity.push.update.disable"	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unity.push.update.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unity-taskbar

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unity.taskbar.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unity.taskbar.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unity.taskbar.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unity-unityactive

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unityActive.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unityActive.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unityActive.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unityActive.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unityActive.disable" -value $True

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-unity-windowcontents

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.unity.windowContents.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.unity.windowContents.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.unity.windowContents.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" -value $True

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-versionget

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.vmxDnDVersionGet.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.vmxDnDVersionGet.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.vmxDnDVersionGet.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-unexposed-features-versionset

Disable certain unexposed features

Vulnerability Procedure:
Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host.

Negative Functional Impact (if applicable)
Some automated tools and process may cease to function

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.guestDnDVersionSet.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.guestDnDVersionSet.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.guestDnDVersionSet.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-vix-messages

Disable VIX messages from the VM

Vulnerability Procedure:
The VIX API is a library for writing scripts and programs to manipulate virtual machines. If you do not make use of custom VIX programming in your environment, then you should consider disabling certain features to reduce the potential for vulnerabilities. The ability to send messages from the VM to the host is one of these features. Note that disabling this feature does NOT adversely affect the functioning of VIX operations that originate outside the guest, so certain VMware and 3rd party solutions that rely upon this capability should continue to work. This is a deprecated interface. Enabling this setting is for Profile 1 only, to ensure that any deprecated interface is turned off for audit purposes.

Negative Functional Impact (if applicable)
Guest will no longer be able to send messages via VIX API

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.vixMessage.disable	1

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.vixMessage.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.vixMessage.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.vixMessage.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.vixMessage.disable" -value $true

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.disable-VMtools-autoinstall

Disable tools auto install

Vulnerability Procedure:

Tools auto install can initiate an automatic reboot, disabling this option will prevent tools from being installed automatically and prevents automatic machine reboots.
For Linux-based operating system, Open VM Tools is widely available as an distribution-based package. Consider using this method to manage your VM Tools installation. If you do this, you should disable VM Tools auto-install using this guideline.

Negative Functional Impact (if applicable)

This option disables tools auto install, all tools installs will have to be manually started.

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.tools.autoInstall.disable	1,2

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.tools.autoInstall.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.tools.autoInstall.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.tools.autoInstall.disable"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.tools.autoInstall.disable" -value $true

Reference Documentation:

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.limit-setinfo-size

Limit informational messages from the VM to the VMX file

Vulnerability Procedure:

The configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value if necessary. You might increase this value if large amounts of custom information are being stored in the configuration file. The default limit is 1MB;this limit is applied even when the sizeLimit parameter is not listed in the .vmx file. Uncontrolled size for the VMX file can lead to denial of service if the datastore is filled.

Negative Functional Impact (if applicable)

None

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
1048576	Null	N/A

Configuration Parameters	Risk Profile
tools.setInfo.sizeLimit	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "tools.setInfo.sizeLimit" [VMX}	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo tools.setInfo.sizeLimit	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "tools.setInfo.sizeLimit" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "tools.setInfo.sizeLimit" -value 1048576

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vm_admin.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-91BF834E-CB92-4014-8CF7-29CE40F3E8A3.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.minimize-console-VNC-use

Control access to VM console via VNC protocol

Vulnerability Procedure:
The VM console enables you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show. This console is also availabe via the VNC protocol. Setting up this access also involves setting up firewall rules on each ESXi server the virtual machine will run on.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
FALSE	Null	N/A

Configuration Parameters	Risk Profile
RemoteDisplay.vnc.enabled	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "RemoteDisplay.vnc.enabled" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo RemoteDisplay.vnc.enabled	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "RemoteDisplay.vnc.enabled" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "RemoteDisplay.vnc.enabled" -value $false

Reference Documentation:

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.prevent-device-interaction-connect

Prevent unauthorized removal, connection and modification of devices

Vulnerability Procedure:

In a virtual machine, users and processes without root or administrator privileges can connect or disconnect devices, such as network adaptors and CD-ROM drives, and can modify device settings. Use the virtual machine settings editor or configuration editor to remove unneeded or unused hardware devices. If you want to use the device again, you can prevent a user or running process in the virtual machine from connecting, disconnecting, or modifying a device from within the guest operating system. By default, a rogue user with nonadministrator privileges in a virtual machine can:

1. Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive
2. Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service
3. Modify settings on a device

Negative Functional Impact (if applicable)

Device interaction is blocked inside the guest OS using VMware tools

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.device.connectable.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.device.connectable.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.device.connectable.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.device.connectable.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.device.connectable.disable" -value $true

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vm_admin.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-F88A5FED-552B-44F9-A168-C62D9306DBD6.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VM.prevent-device-interaction-edit

Prevent unauthorized removal, connection and modification of devices

Vulnerability Procedure:

In a virtual machine, users and processes without root or administrator privileges can connect or disconnect devices, such as network adaptors and CD-ROM drives, and can modify device settings. Use the virtual machine settings editor or configuration editor to remove unneeded or unused hardware devices. If you want to use the device again, you can prevent a user or running process in the virtual machine from connecting, disconnecting, or modifying a device from within the guest operating system. By default, a rogue user with nonadministrator privileges in a virtual machine can:

1. Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive
2. Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service
3. Modify settings on a device

Negative Functional Impact (if applicable)

Device interaction is blocked inside the guest OS using VMware tools

Web Client Assessment Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
TRUE	Null	N/A

Configuration Parameters	Risk Profile
isolation.device.edit.disable	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "isolation.device.edit.disable" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo isolation.device.edit.disable	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "isolation.device.edit.disable" | Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "isolation.device.edit.disable" -value $true

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-F88A5FED-552B-44F9-A168-C62D9306DBD6.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.restrict-host-info

Do not send host information to guests

Vulnerability Procedure:
By enabling a VM to get detailed information about the physical host, an adversary could potentially use this information to inform further attacks on the host.
If set to True a VM can obtain detailed information about the physical host. *The default value for the parameter is False but is displayed as Null. Setting to False is purely for audit purposes.*
This setting should not be TRUE unless a particular VM requires this information for performance monitoring.

Negative Functional Impact (if applicable)
Unable to retrieve performance information about the host from inside the guest, there are times when this can be useful for troubleshooting.

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
False	Null	N/A

Configuration Parameters	Risk Profile
tools.guestlib.enableHostInfo	1,2

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "tools.guestlib.enableHostInfo" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo tools.guestlib.enableHostInfo	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "tools.guestlib.enableHostInfo"| Select Entity, Name, Value	# Add the setting to all VMs Get-VM | New-AdvancedSetting -Name "tools.guestlib.enableHostInfo" -value $false

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-2CF880DA-2435-4201-9AFB-A16A11951A2D.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VM.TransparentPageSharing-inter-VM-Enabled

Check for enablement of salted VM's that are sharing memory pages

Vulnerability Procedure:

When salting is enabled (Mem.ShareForceSalting=1 or 2) in order to share a page between two virtual machines both salt and the content of the page must be same. A salt value is a configurable vmx option for each virtual machine. You can manually specify the salt values in the virtual machine's vmx file with the new vmx option sched.mem.pshare.salt. If this option is not present in the virtual machine's vmx file, then the value of vc.uuid vmx option is taken as the default value. Since the vc.uuid is unique to each virtual machine, by default TPS happens only among the pages belonging to a particular virtual machine (Intra-VM).
If a group of virtual machines are considered trustworthy, it is possible to share pages among them by setting a common salt value for all those virtual machines (inter-VM).

Negative Functional Impact (if applicable)

Running with Inter-VM page sharing should only be done between virtual machines that are trust-worthy.

Web Client Assessment Procedure:

From the vSphere Web Client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.
If there is a non-null value and that value is common to more than one virtual machine, those virtual machines have inter-VM TPS enabled.

Web Client Remediation Procedure:

From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options".
Click "Edit".
Go to "VM Options" tab and expand "Advanced".
Click on "Edit Configuration".
Click on "Add Row" and then edit the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
Site-Specific	Null	NO

Configuration Parameters	Risk Profile
sched.mem.pshare.salt	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "sched.mem.pshare.salt" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
vmware-cmd --server [SERVER] --username [USERNAME] --password [PASSWORD] /vmfs/volumes/[DATASTORE]/[VM]/[VM].vmx getguestinfo sched.mem.pshare.salt	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "sched.mem.pshare.salt"| Select Entity, Name, Value	# Add the setting to all VMs $ vmsaltvalue = "<some unique value>" Get-VM | New-AdvancedSetting -Name "sched.mem.pshare.salt" -value $vmsaltvalue

Reference Documentation:

https://kb.vmware.com/kb/2080735
https://kb.vmware.com/kb/2097593
https://kb.vmware.com/kb/2091682

vSphere API:

VM.verify-network-filter

Control access to VMs through the dvfilter network APIs

Vulnerability Procedure:
An attacker might compromise a VM by making use the dvFilter API. Configure only those VMs to use the API that need this access.
This setting is considered an "Audit Only" guideline. If there is a value present, the admin should check it to ensure it is correct.

Negative Functional Impact (if applicable)
incorrectly configuring this option can negatively impact functionality of tools that use dvFilter API's.

Web Client Assessment Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that the desired configuration parameter is present with the desired value.
If a VM is not supposed to be protected by a product using the dvfilter API, ensure that the following is not present in its VMX file: ethernet0.filter1.name = dv-filter1where “ethernet0” is the network adaptor interface of the virtual machine that is to be protected, “filter1” is the number of the filter that is being used, and “dv-filter1” is the name of the particular data path kernel module that is protecting the VM. If the VM is supposed to be protected, ensure that the name of the data path kernel is set correctly.

Web Client Remediation Procedure:
From the vSphere web client, select each VM and click "Manage" -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add the desired configuration parameter with the desired value.

Desired Value	Default Value	Able to set via Host Profiles
Null unless using dvfilter	Null	N/A

Configuration Parameters	Risk Profile
ethernetn.filtern.name = filtername	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
grep -i "^ethernet[0-9]*.filter[0-9]*.name" [VMX]	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
1. vifs --server [SERVER] --username [USERNAME] --password [PASSWORD] -g "[DATASTORE] VM/VM.vmx" VM.vmx 2. grep -i "^ethernet[0-9]*.filter[0-9]*.name" [VMX]	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List the VMs and their current settings Get-VM | Get-AdvancedSetting -Name "ethernet*.filter*.name*" | Select Entity, Name, Value	

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Reference Documentation:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionValue.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vNetwork.enable-bpdu-filter

Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled

Vulnerability Procedure:
BPDU Guard and Portfast are commonly enabled on the physical switch to which the ESXi host is directly connected to reduce the STP convergence delay. If a BPDU packet is sent from a virtual machine on the ESXi host to the physical switch so configured, a cascading lockout of all the uplink interfaces from the ESXi host can occur. To prevent this type of lockout, BPDU Filter can be enabled on the ESXi host to drop any BPDU packets being sent to the physical switch. The caveat is that certain SSL VPN which use Windows bridging capability can legitimately generate BPDU packets. The administrator should verify that there are no legitimate BPDU packets generated by virtual machines on the ESXi host prior to enabling BPDU Filter. If BPDU Filter is enabled in this situation, enabling Reject Forged Transmits on the virtual switch port group adds protection against Spanning Tree loops.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From vSphere Web Client, select the host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Net.BlockGuestBPDU to see the configured value. It should be set to the desired value.

Web Client Remediation Procedure:
From vSphere Web cClient, select the host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Net.BlockGuestBPDU to see the configured value. Click edit and set it to the desired value.

Desired Value	Default Value	Able to set via Host Profiles
1	0	N/A

Configuration Parameters	Risk Profile
Net.BlockGuestBPDU	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
esxcli system settings advanced list -o /Net/BlockGuestBPDU	esxcli system settings advanced set -o /Net/BlockGuestBPDU -i 0

vCLI Shell Command Assessment	VCLI Shell Command Remediation
esxcli <conn_options> system settings advanced list -o /Net/BlockGuestBPDU	esxcli conn_options system settings advanced set -o /Net/BlockGuestBPDU -i 0

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:
http://kb.vmware.com/kb/2017193
http://kb.vmware.com/kb/2047822
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-FA661AE0-C0B5-4522-951D-A3790DBE70B4.html

vmware
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html

vNetwork.limit-network-healthcheck

Enable VDS network healthcheck only if you need it

Vulnerability Procedure:
Network Healthcheck is disabled by default. Once enabled, the healthcheck packets contain information on host#, vds# port#, which an attacker would find useful. It is recommended that network healthcheck be used for troubleshooting, and turned off when troubleshooting is finished.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From the vSphere Web Client, select each VDS and go to "Manage" -> "Settings" -> Health check". Verify that "VLAN and MTU Check" and "Teaming and Failover Check" are both "Disabled".

Web Client Remediation Procedure:
From the vSphere Web Client, select each VDS and go to "Manage" -> "Settings" -> Health check". Click "Edit" and set "VLAN and MTU Check" and "Teaming and Failover Check" to "Disabled".

Desired Value	Default Value	Able to set via Host Profiles
Disabled	Disabled	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-C590B7D3-4E28-4F2B-8A59-4CDB9C6F2DAA.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-4A6C1E1C-8577-4AE6-8459-EEB942779A82.html

vSphere API:
http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.wssdk.apiref.doc%2Fvim.DistributedVirtualSwitch.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vNetwork.reject-forged-transmit

Ensure that the “Forged Transmits” policy is set to reject

Vulnerability Procedure:

If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.
Forged transmissions is set to Accept by default.
This means the virtual switch does not compare the source and effective MAC addresses.
To protect against MAC address impersonation, all virtual switches should have forged transmissions set to Reject. Reject Forged Transmit can be set at the vSwitch and/or the Portgroup level. You can override switch level settings at the Portgroup level.

Negative Functional Impact (if applicable)

This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This

Web Client Assessment Procedure:

From the vSphere Web Client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click edit. Go to "Security" and verify that "Forged Transmits" is set to "Reject".

Web Client Remediation Procedure:

From the vSphere Web Client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click edit. Go to "Security" and set the "Forged Transmits" to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Accept	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli network vswitch standard policy security get -v [VSWITCH]	# esxcli network vswitch standard policy security set -v vSwitch2 -f false

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> network vswitch standard policy security get -v [VSWITCH]	# esxcli conn_options vswitch standard policy security set -v vSwitch2 -f false

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all vSwitches and their Security Settings Get-VirtualSwitch -Standard | Select VMHost, Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" } Else { "Reject"} }}, `	

@{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) { "Accept" } Else { "Reject"} }}, ` @{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-7DC6486F-5400-44DF-8A62-6273798A2F80.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.host.NetworkPolicy.SecurityPolicy.html

vNetwork.reject-forged-transmit-dvportgroup

Ensure that the “Forged Transmits” policy is set to reject

Vulnerability Procedure:

If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.
When the Forged transmits option is set to Accept, ESXi does not compare source and effective MAC addresses.
To protect against MAC impersonation, you can set the Forged transmits option to Reject. If you do, the host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to see if they match. If the addresses do not match, the ESXi host drops the packet.

Negative Functional Impact (if applicable)

This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality.
An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address.

Web Client Assessment Procedure:

From vSphere web client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies". Verify that "Forged transmits" policy is set to "Reject".

Web Client Remediation Procedure:

From vSphere Web Client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies" and click "Edit". Go to "Security" and set the "Forged transmits" policy to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Reject	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all dvPortGroups and their Security Settings Get-VirtualPortGroup -Distributed | Select Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept" } Else { "Reject"} }}, ` @{N="PromiscuousMode";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) { "Accept" } Else { "Reject"} }}, ` @{N="ForgedTransmits";E={if	

($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-C590B7D3-4E28-4F2B-8A59-4CDB9C6F2DAA.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.dvs.VmwareDistributedVirtualSwitch.VMwarePortgroupPolicy.html

vNetwork.reject-mac-changes

Ensure that the “MAC Address Changes” policy is set to reject

Vulnerability Procedure:

If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the port groups that these applications are connected to. Reject MAC Changes can be set at the vSwitch and/or the Portgroup level. You can override switch level settings at the Portgroup level.

Negative Functional Impact (if applicable)

This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This w

Web Client Assessment Procedure:

From the vSphere web client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click edit. Go to "Security" and verify that "MAC address changes" is set to "Reject".

Web Client Remediation Procedure:

From the vSphere web client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click edit. Go to "Security" and set the "MAC address changes" to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Accept	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli network vswitch standard policy security get -v [VSWITCH]	# esxcli network vswitch standard policy security set -v vSwitch2 -m false

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> network vswitch standard policy security get -v [VSWITCH]	# esxcli conn_options vswitch standard policy security set -v vSwitch2 -m false

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all vSwitches and their Security Settings Get-VirtualSwitch -Standard | Select VMHost, Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" } Else { "Reject"} }}, `	

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

@{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) { "Accept" } Else { "Reject"} }}, ` @{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-942BD3AA-731B-4A05-8196-66F2B4BF1ACB.html

vSphere API:

http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.host.NetworkPolicy.SecurityPolicy.html

vNetwork.reject-mac-changes-dvportgroup

Ensure that the “MAC Address Changes” policy is set to reject

Vulnerability Procedure:

If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the dvPortgroups that these applications are connected to.

Negative Functional Impact (if applicable)

This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This w

Web Client Assessment Procedure:

From vSphere web client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies". Verify that "MAC address changes" policy is set to "Reject".

Web Client Remediation Procedure:

From vSphere web client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies" and click "Edit". Go to "Security" and set the "MAC address changes" policy to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Reject	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all dvPortGroups and their Security Settings Get-VirtualPortGroup -Distributed | Select Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept" } Else { "Reject"} }}, ` @{N="PromiscuousMode";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) { "Accept" } Else { "Reject"} }}, ` @{N="ForgedTransmits";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-C590B7D3-4E28-4F2B-8A59-4CDB9C6F2DAA.html

vSphere API:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.dvs.VMwareDistributedVirtualSwitch.SecurityPolicy.html

vNetwork.reject-promiscuous-mode

Ensure that the “Promiscuous Mode” policy is set to reject

Vulnerability Procedure:

When promiscuous mode is enabled for a virtual switch all virtual machines connected to the Portgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that Portgroup. Promiscuous mode is disabled by default on the ESXI Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons. Security devices might require the ability to see all packets on a vSwitch. An exception should be made for the Portgroups that these applications are connected to, in order to allow for full-time visibility to the traffic on that Portgroup. Promiscous mode can be set at the vSwitch and/or the Portgroup level. You can override switch level settings at the Portgroup level.

Negative Functional Impact (if applicable)

Security devices that require the ability to see all packets on a vSwitch will not operate properly if the “Promiscuous Mode” policy is set to “Reject".

Web Client Assessment Procedure:

From the vSphere Web Client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click edit. Go to "Security" and verify that "Promiscuous Mode" is set to "Reject".

Web Client Remediation Procedure:

From the vSphere Web Client select the host and click "Manage" -> "Networking" -> "Virtual Switches". For each virtual switch and for each port group within that virtual switch, click Edit. Go to "Security" and set the "Promiscuous Mode" to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Reject	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli network vswitch standard policy security get -v [VSWITCH]	# esxcli network vswitch standard policy security set -v vSwitch2 -p false

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> network vswitch standard policy security get -v [VSWITCH]	# esxcli conn_options vswitch standard policy security set -v vSwitch2 -p false

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all vSwitches and their Security Settings Get-VirtualSwitch -Standard | Select VMHost, Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" } Else { "Reject"} }}, ` @{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) { "Accept" } Else { "Reject"} }}, `	

@{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-92F3AB1F-B4C5-4F25-A010-8820D7250350.html

vSphere API:

http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.host.NetworkPolicy.SecurityPolicy.html

vNetwork.reject-promiscuous-mode-dvportgroup

Ensure that the “Promiscuous Mode” policy is set to reject

Vulnerability Procedure:

When promiscuous mode is enabled for a dvPortgroup, all virtual machines connected to the dvPortgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that dvPortgroup. Promiscuous mode is disabled by default on the ESXI Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons. Security devices might require the ability to see all packets on a vSwitch. An exception should be made for the dvPortgroups that these applications are connected to, in order to allow for full-time visibility to the traffic on that dvPortgroup. Unlike standard vSwitches, dvSwitches only allow Promiscuous Mode at the dvPortgroup level

Negative Functional Impact (if applicable)

Security devices that require the ability to see all packets on a vSwitch will not operate properly if the “Promiscuous Mode” parameter is set to “Reject.”

Web Client Assessment Procedure:

From vSphere web client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies". Verify that "Promiscuous Mode" policy is set to "Reject".

Web Client Remediation Procedure:

From vSphere web client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Policies" and click "Edit". Go to "Security" and set the "Promiscuous Mode" policy to "Reject".

Desired Value	Default Value	Able to set via Host Profiles
Reject	Reject	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
# List all dvPortGroups and their Security Settings Get-VirtualPortGroup -Distributed | Select Name, ` @{N="MacChanges";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept" } Else { "Reject"} }}, ` @{N="PromiscuousMode";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) { "Accept" } Else { "Reject"} }}, ` @{N="ForgedTransmits";E={if ($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) { "Accept" } Else { "Reject"} }}	

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-C590B7D3-4E28-4F2B-8A59-4CDB9C6F2DAA.html

vSphere API:

http://pubs.vmware.com/vsphere-55/topic/com.vmware.wssdk.apiref.doc/vim.dvs.VMwareDistributedVirtualSwitch.SecurityPolicy.html

vNetwork.restrict-netflow-usage

Ensure that VDS Netflow traffic is only being sent to authorized collector IPs

Vulnerability Procedure:
The vSphere VDS can export Netflow information about traffic crossing the VDS. Netflow exports are not encrypted and can contain information about the virtual network making it easier for a MITM attack to be executed successfully. If Netflow export is required, verify that all VDS Netflow target IP's are correct.

Negative Functional Impact (if applicable)
None

Web Client Assessment Procedure:
From vSphere Web Client, for each distributed switch go to "Manage" -> "Settings" -> "NetFlow". Verify that "Collector IP address" and "Collector port" are legitimate.

Web Client Remediation Procedure:
From vSphere Web Client, for each distributed switch go to "Manage" -> "Settings" -> "NetFlow". Click "Edit" and set the "Collector IP address" and "Collector port" as appropriate.

Desired Value	Default Value	Able to set via Host Profiles
Site-Specific	Null	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation
Get-VDPortgroup | Select Name, VirtualSwitch, @{Name="NetflowEnabled";Expression={$_.Extensiondata.Config.defaultPortConfig.ipfixEnabled.Value}} \| Where-Object {$_.NetflowEnabled -eq "True"}	# Disable Netfow for a VDPortgroup $DPortgroup = <name of portgroup> Get-VDPortgroup $DPortGroup | Disable-PGNetflow

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-FA661AE0-C0B5-4522-951D-A3790DBE70B4.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-55FCEC92-74B9-4E5F-ACC0-4EA1C36F397A.html

vSphere API:

http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.wssdk.apiref.doc%2Fvim.DistributedVirtualSwitch.html

vNetwork.restrict-port-level-overrides

Restrict port-level configuration overrides on VDS

Vulnerability Procedure:
Port-level configuration overrides are disabled by default. Once enabled, this allows for different security settings to be set from what is established at the Port-Group level. There are cases where particular VM's require unique configurations, but this should be monitored so it is only used when authorized. If overrides are not monitored, anyone who gains access to a VM with a less secure VDS configuration could surreptiously exploit that broader access.

Negative Functional Impact (if applicable)
Specific port level overrides would be denied.

Web Client Assessment Procedure:
From vSphere Web Client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Properties". Verify that all "Override port policies" are "Disabled".

Web Client Remediation Procedure:
From vSphere Web Client, for each portgroup within each distributed switch go to "Manage" -> "Settings" -> "Properties". Click "Edit" and go to "Advanced". Disable all "Override port policies".

Desired Value	Default Value	Able to set via Host Profiles
Disabled	Disabled	N/A

Configuration Parameters	Risk Profile
N/A	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
N/A	N/A

vCLI Shell Command Assessment	VCLI Shell Command Remediation
N/A	N/A

PowerCLI Command Assessment	PowerCLI Command Remediation

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-FA661AE0-C0B5-4522-951D-A3790DBE70B4.html
http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-DDF5CD98-454A-471D-9053-03ABB8FE86D1.html

vSphere API:
http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.wssdk.apiref.doc%2Fvim.DistributedVirtualSwitch.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vNetwork.verify-dvfilter-bind

Prevent unintended use of dvfilter network APIs

Vulnerability Procedure:

If you are not using products that make use of the dvfilter network API, the host should not be configured to send network information to a VM. If the API is enabled, an attacker might attempt to connect a VM to it, thereby potentially providing access to the network of other VMs on the host. If you are using a product that makes use of this API then verify that the host has been configured correctly.

Negative Functional Impact (if applicable)

This will prevent a dvfilter-based network security appliance from functioning

Web Client Assessment Procedure:

From vSphere web client, select a host and click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Net.DVFilterBindIpAddress to see the configured value. It should be set to the desired value or to the IP address of the appropriate VM using dvfilter network APIs.

Web Client Remediation Procedure:

From vSphere web client, select host and then click "Manage" -> "Settings" -> "System" -> "Advanced System settings". Filter for Net.DVFilterBindIpAddress to see the configured value. Click edit and set it to the desired value or to the IP address of the appropriate VM using dvfilter network APIs.

Desired Value	Default Value	Able to set via Host Profiles
Null	Null	NO

Configuration Parameters	Risk Profile
Net.DVFilterBindIpAddress	1,2,3

ESXi Shell Command Assessment	ESXi Shell Command Remediation
# esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /Net/DVFilterBindIpAddress	# esxcli system settings advanced set -o /Net/DVFilterBindIpAddress -d

vCLI Shell Command Assessment	VCLI Shell Command Remediation
# esxcli <conn_options> --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /Net/DVFilterBindIpAddress	# esxcli conn_options system settings advanced set -o /Net/DVFilterBindIpAddress -d

PowerCLI Command Assessment	PowerCLI Command Remediation
# List Net.DVFilterBindIpAddress for each host Get-VMHost | Select Name, @{N="Net.DVFilterBindIpAddress";E={$_ | Get-VMHostAdvancedConfiguration Net.DVFilterBindIpAddress | Select -ExpandProperty Values}}	# Set Remove Net.DVFilterBindIpAddress to null on all hosts Get-VMHost HOST1 | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name Net.DVFilterBindIpAddress -Value "" }

Reference Documentation:

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.ext_solutions.doc/GUID-6013E15D-92CE-4970-953C-ACCB36ADA8AD.html

vSphere API:
http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.apiref.doc/vim.option.OptionManager.html