RED Check

REPORT

Report number	*198da1d1-49b4-4a57-a6df-20a2621d048c*
Profile	*Compliance*
Job	*Job_4109*
Start/stop scanning	*29.05.2017 14:34:39 / 29.05.2017 14:35:22*
Report generation	*29.05.2017 14:37:19*
Name	*Quick_192.168.130.130_4*
Description	*Autogenerated report from history tab for "192.168.130.130" target of "Job_4109" job.*
Targets [1]	*192.168.130.130*

Scan result summary table

Target	Benchmark	Total	Success
192.168.130.130	VMware ESXi Server 6 Compliance	65	13

Target: 192.168.130.130

Start/stop scanning	*29.05.2017 14:34:39 / 29.05.2017 14:35:22*
Credentials	*Profile name: vmware 6.5* *Type: VMware*
Data retrieving method	*Agentless*

VMware ESXi Server 6 Compliance

The compliance doesn't match the reference. Total - 65, success - 13 (20 %)

✓ **Pass (13)** ✗ **Fail (12)** ✎ **Not Applicable (39)**
⏸ **Not Checked (1)**

- ✗ **VMware ESXi Server**
  - ✗ **ESXi hosts**
    - ✗ Enable Strict Lockdown mode to restrict access
    - ✗ Verify Image Profile and VIB Acceptance Levels is VMware Certified
    - ✗ Audit the list of users who are on the Exception Users List and whether the have administrator privleges
    - ✗ Configure NTP time synchronization
    - ✗ Configure persistent logging for all ESXi host
    - ✓ Ensure proper SNMP configuration
    - ✓ Disable Managed Object Browser (MOB)
    - ✗ Use Active Directory for local user authentication
    - ✗ Configure remote logging for ESXi hosts
    - ✓ Disable SSH service
    - ✓ Disable ESXi Shell service
    - ✗ Configure the ESXi host firewall to restrict access to services running on the host
    - ✓ Set the time after which a locked account is automatically unlocked
    - ✗ Set the count of maximum failed login attempts before the account is locked out
    - ✓ Set DCUI.Access to allow trusted users to override lockdown mode
    - ✓ Audit DCUI timeout value
    - ✓ Establish a password policy for password complexity
    - ✓ Set a timeout to automatically terminate idle ESXi Shell and SSH sessions
    - ✓ Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run
    - ✓ Ensure default setting for intra-VM TPS is correct
    - ⏸ Keep ESXi system properly patched
  - ✎ **VM**
    - ✎ **Explicitly disable copy/paste operations**
      - ✎ Disable copy operations
      - ✎ Disable dnd operations
      - ✎ Disable setGUIOptions
      - ✎ Disable paste operations
    - ✎ **Disable virtual disk shrinking**
      - ✎ Disable virtual disk shrink
      - ✎ Disable virtual disk wiper
    - ✎ **Disable certain unexposed features**
      - ✎ Disable autologon feature
      - ✎ Disable biosbbs feature

        - ✎ Disable getcreds feature
        - ✎ Disable launchmenu feature
        - ✎ Disable memsfss features
        - ✎ Disable protocolhandler feature
        - ✎ Disable shellaction feature
        - ✎ Disable toporequest feature
        - ✎ Disable trashfolderstate feature
        - ✎ Disable trayicon feature
        - ✎ Disable unity feature
        - ✎ Disable unity interlock features
        - ✎ Disable unitypush feature
        - ✎ Disable unity taskbar feature
        - ✎ Disable unity unityactive feature
        - ✎ Disable unity windowcontents feature
        - ✎ Disable versionget feature
        - ✎ Disable versionset feature
    - ✎ **Disconnect unauthorized devices**
        - ✎ Disconnect floppy devices
        - ✎ Disconnect parallel devices
        - ✎ Disconnect serial devices
    - ✎ **Prevent unauthorized removal, connection and modification of devices**
        - ✎ Prevent device interaction connection
        - ✎ Prevent unauthorized modification of devices
    - ✎ Disable HGFS file transfers
    - ✎ Avoid using independent nonpersistent disks
    - ✎ Disable VIX messages from the VM
    - ✎ Disable tools auto install
    - ✎ Limit informational messages from the VM to the VMX file
    - ✎ Control access to VM console via VNC protocol
    - ✎ Do not send host information to guests
    - ✎ Check for enablement of salted VM's that are sharing memory pages
    - ✎ Control access to VMs through the dvfilter network APIs
    - ✎ Audit all uses of PCI or PCIe passthrough functionality
- ☒ **vNetwork**
    - ☒ Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled
    - ☒ Ensure that the “Forged Transmits” policy is set to reject
    - ☒ Ensure that the “MAC Address Changes” policy is set to reject
    - ✓ Ensure that the “Promiscuous Mode” policy is set to reject
    - ✓ Prevent unintended use of dvfilter network APIs

Parameters description

Group	
Title	**VMware ESXi Server**
Description	

VMware ESXi Server is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that one installs in an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel.

Group	
Title	**ESXi hosts**
Description	

ESXi hosts configuration privileges control the ability to configure hosts.

Parameter	Severity: High
Title	**Enable Strict Lockdown mode to restrict access**
Description	

Reference value: **Strict**

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.

Remediation

From the VMware vSphere web client, select host and click on "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Security Profile". Scroll down to "Lockdown Mode". Click "Edit" and then choose "Strict".

Parameter	Severity: High
Title	**Verify Image Profile and VIB Acceptance Levels is VMware Certified**
Description	

Reference value: **VMware Certified**

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.

Remediation

From VMware vSphere web client, select host and then click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Security Profile". Пролистайте до you see "Host Image Profile Acceptance Level". Click "Edit" and set the "Acceptance Level" parameter to "VMware Certified".

Parameter	Severity: High
Title	**Audit the list of users who are on the Exception Users List and whether the have administrator privleges**
Description	

Reference value: **Site-specific**

In VMware vSphere 6.0 and later, you can add users to the Exception Users list from the VMware 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.

Remediation

From the VMware vSphere web client, select host and click on "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Security Profile". Пролистайте до "Lockdown Mode". Click "Edit" and then click on "Exception Users". Add or delete users as per your site requirements.

Parameter	Severity: High
Title	**Configure NTP time synchronization**
Description	

Reference value: **Site Specific**

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.

Remediation

In the VMware 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.

Parameter	Severity: High
Title	**Configure persistent logging for all ESXi host**
Description	

Reference value: **Site Specific**

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.

Remediation

1. Identify the datastore path where you want to place scratch, then login to the VMware vSphere Web Client. 2. Navigating to the host and select "Manage" ("Configure" in 6.5) 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.

Parameter	Severity: High
Title	**Ensure proper SNMP configuration**

Description

Reference value: **site-specific**

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.

Remediation

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

Parameter Severity: High

Title **Disable Managed Object Browser (MOB)**

Description

Reference value: **False**

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 VMware vSphere SDK. In Sphere 6.0 this is disabled by default

Remediation

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.

Parameter Severity: High

Title **Use Active Directory for local user authentication**

Description

Reference value: **N/A**

Join ESXi hosts to an Active Directory (AD) domain to eliminate the need to create and maintain multiple local user accounts. Using AD for user authentication simplifies the ESXi host configuration, ensures password complexity and reuse policies are enforced and reduces the risk of security breaches and unauthorized access. Note: if the AD group "ESX Admins" (default) exists then all users and groups that are assigned as members to this group will have full administrative access to all ESXi hosts the domain.

Remediation

From the VMware vSphere Web Client, select the host and go to "Manage" ("Configure" in 6.5) -> "Authentication Services" and click the "Join Domain" button. Provide the domain name along with the user credentials for an AD user that has the rights to join computers to the domain. Notes: (1) you can use Host Profiles to automate adding hosts to an AD domain. (2) Consider using the VMware vSphere Authentication proxy to avoid transmitting AD credentials over the network. Refer to the "enable-auth-proxy" recommendation for more information.

Parameter Severity: High

Title **Configure remote logging for ESXi hosts**

Description

Reference value: **Site Specific**

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 VMware vSphere Syslog Collector.

Remediation

Step 1: Install/Enable a syslog host (vSphere Syslog Collector recommended). Step 2: From the VMware vSphere Web Client select the host and click "Manage" ("Configure" in 6.5) -> "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.

Parameter Severity: High

Title **Disable SSH service**

Description

Reference value: **False**

This service is disabled by default

Remediation

From the VMware vSphere web client, select host and click on "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Security Profile". Пролистайте до "Services".Click "Edit" and then click on "SSH". Choose button "stop".

Parameter Severity: High

Title **Disable ESXi Shell service**

Description

Reference value: **False**

This service is disabled by default

Remediation

From the VMware vSphere web client, select host and click on "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Security Profile". Пролистайте до "Services".Click "Edit" and then click on "ESXi Shell". Choose button "stop".

Parameter Severity: High

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

Description

Reference value: **Site Specific**

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.

Remediation

From the VMware vSphere web client, select the host and click "Manage" ("Configure" in 6.5) -> "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.

Parameter Severity: High

Title **Set the time after which a locked account is automatically unlocked**

Description

Reference value: **900**

Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account after reaching a threshold.

In case, you would want to auto unlock the account, i.e. unlock the account without administrative action, set the time for which the account remains locked. Setting a high duration for which account remains locked would deter and serverly slow down the brute force method of logging in.

Remediation

From the VMware vSphere Web Client select the host, click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced Sytem Settings". Enter "Security.AccountUnlockTime" in the filter. Click edit and set the value for this parameter to 900.

Parameter Severity: High

Title **Set the count of maximum failed login attempts before the account is locked out**

Description

Reference value: **3**

Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account after reaching a threshold.

Remediation

From the VMware vSphere Web Client select the host, click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced Sytem Settings". Enter "Security.AccountLockFailures" in the filter. Click edit and set the value for this parameter to 3.

Parameter Severity: High

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

Description

Reference value: **List of authorized users**

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.

Remediation

From the VMware vSphere Web Client select the host, click "Manage" ("Configure" in 6.5) -> "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.

Parameter Severity: High

Title **Audit DCUI timeout value**

Description

Reference value: **600**

DCUI is used for directly logging into ESXi host and carrying out host management tasks. The idle connections to DCUI must be terminated to avoid any unintended usage of the DCUI originating from a left over login session.

Remediation

From the VMware vSphere Web Client select the host, click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced Sytem Settings". Enter "UserVars.DcuiTimeOut" in the filter. Click edit and set the value for this parameter to 600 or more restrictive.

Parameter Severity: High

Title **Establish a password policy for password complexity**

Description

Reference value: **Site specific**

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.

Remediation

From VMware vSphere web client, select host and then click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced System settings". Filter for Security.PasswordQualityControl to see the configured value. Set it to the default value or more restrictive.

🟥 **Parameter** Severity: High

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

Description

Reference value: **900**

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.

Remediation

From VMware vSphere web client, select host and then click "Manage" ("Configure" in 6.5) -> "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.

🟥 **Parameter** Severity: High

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

Description

Reference value: **900**

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.

Remediation

From VMware vSphere web client, select host and then click "Manage" ("Configure" in 6.5) -> "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.

🟥 **Parameter** Severity: High

Title **Ensure default setting for intra-VM TPS is correct**

Description

Reference value: **2**

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.

Remediation

From VMware vSphere Web Client, select a host and then click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced System settings". Filter for Mem.ShareForceSalting. Click edit and set it to 2.

Parameter Severity: High

Title **Keep ESXi system properly patched**

Description

Reference value: **NA**

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.

Remediation

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

Group

Title **VM**

Description

VirtualMachine is the managed object type for manipulating virtual machines, including templates that can be deployed (repeatedly) as new virtual machines. This type provides methods for configuring and controlling a virtual machine.
VirtualMachine extends the ManagedEntity type because virtual machines are part of a virtual infrastructure inventory. The parent of a virtual machine must be a folder, and a virtual machine has no children.
Destroying a virtual machine disposes of all associated storage, including the virtual disks. To remove a virtual machine while retaining its virtual disk storage, a client must remove the virtual disks from the virtual machine before destroying it.

If this section is not applicable than there is no virtual machine on ESXi host.

Group

Title **Explicitly disable copy/paste operations**

Description

Explicitly disable copy/paste operations

Parameter Severity: High

Title **Disable copy operations**

Description

Reference value: **True**

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

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.copy.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable dnd operations**

Description

Reference value: **True**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.dnd.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable setGUIOptions**

Description

Reference value: **FALSE**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.setGUIOptions.enable" parameter with the value "false".

Parameter Severity: High

Title **Disable paste operations**

Description

Reference value: **True**

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

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.paste.disable" parameter with the value "true".

Group

Title **Disable virtual disk shrinking**

Description

Disable virtual disk shrinking

Parameter Severity: High

Title **Disable virtual disk shrink**

Description

Reference value: **True**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.diskShrink.disable" parameter with the value "true".

Parameter	Severity: High
Title	**Disable virtual disk wiper**

Description

Reference value: **True**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.diskWiper.disable" parameter with the value "true".

Group	
Title	**Disable certain unexposed features**

Description

Disable certain unexposed features

Parameter	Severity: High
Title	**Disable autologon feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on both VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.ghi.autologon.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable biosbbs feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.bios.bbs.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable getcreds feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.getCreds.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable launchmenu feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.ghi.launchmenu.change" parameter with the value "true".

Parameter Severity: High

Title **Disable memsfss features**

Description

Reference value: **True**

Because VMware virtual machines are designed to work on both VMware vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don’t apply when running on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.memSchedFakeSampleStats.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable protocolhandler feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Expand "Advanced Settings". Scroll the list of "Configuration Parameters" and ensure that "isolation.tools.ghi.protocolhandler.info.disable" parameter is present with the value "true".

Parameter Severity: High

Title **Disable shellaction feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.ghi.host.shellAction.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable toporequest feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.dispTopoRequest.disable" parameter with the value "true".

Parameter Severity: High

Title	**Disable trashfolderstate feature**
Description	

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.trashFolderState.disable" parameter with the value "true".

🟥 **Parameter**	Severity:	High
Title	**Disable trayicon feature**	
Description		

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.ghi.trayicon.disable" parameter with the value "true".

🟥 **Parameter**	Severity:	High
Title	**Disable unity feature**	
Description		

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unity.disable" parameter with the value "true".

🟥 **Parameter**	Severity:	High
Title	**Disable unity interlock features**	
Description		

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click

"Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unityInterlockOperation.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable unitypush feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unity.push.update.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable unity taskbar feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unity.taskbar.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable unity unityactive feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unityActive.disable" parameter with the value "true".

Parameter Severity: High

Title **Disable unity windowcontents feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.unity.windowContents.disable" parameter with the value "true".

🟥 **Parameter**	Severity: High
Title	**Disable versionget feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.vmxDnDVersionGet.disable" parameter with the value "true".

🟥 **Parameter**	Severity: High
Title	**Disable versionset feature**

Description

Reference value: **True**

Some VMX parameters don't apply on VMware vSphere because VMware virtual machines work on VMware 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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.guestDnDVersionSet.disable" parameter with the value "true".

▦ **Group**	
Title	**Disconnect unauthorized devices**

Description

Disconnect unauthorized devices

🟥 **Parameter**	Severity: High
Title	**Disconnect floppy devices**

Description

Reference value: **not present**

Ensure that no floppy device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be

FALSE. NOTE: The parameters listed are not sufficient to ensure that a device is usable; other required parameters specify how each device is instantiated. Any enabled or connected device represents a potential attack channel. When setting is set to FALSE, functionality is disabled, however the device may still show up withing the guest operation system.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Hardware". Click "Edit". Remove floppy device if it existes.

Parameter Severity: High

Title **Disconnect parallel devices**

Description

Reference value: **not present**

Ensure that no parallel device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE. NOTE: The parameters listed are not sufficient to ensure that a device is usable; other required parameters specify how each device is instantiated. Any enabled or connected device represents a potential attack channel. When setting is set to FALSE, functionality is disabled, however the device may still show up withing the guest operation system.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Hardware". Click "Edit". Remove parallel device if it existes.

Parameter Severity: High

Title **Disconnect serial devices**

Description

Reference value: **not present**

Ensure that no serial device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE. NOTE: The parameters listed are not sufficient to ensure that a device is usable; other required parameters specify how each device is instantiated. Any enabled or connected device represents a potential attack channel. When setting is set to FALSE, functionality is disabled, however the device may still show up withing the guest operation system.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Hardware". Click "Edit". Remove serial device if it existes.

Group

Title **Prevent unauthorized removal, connection and modification of devices**

Description

Prevent unauthorized connection of devices

Parameter Severity: High

Title **Prevent device interaction connection**

Description

Reference value: **True**

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

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.device.connectable.disable" parameter with the value "true".

🟥 **Parameter** Severity: High

Title **Prevent unauthorized modification of devices**

Description

Reference value: **True**

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

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.device.edit.disable" parameter with the value "true".

🟥 **Parameter** Severity: High

Title **Disable HGFS file transfers**

Description

Reference value: **True**

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

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.hgfsServerSet.disable" parameter with the value "true".

🟥 **Parameter** Severity: High

Title **Avoid using independent nonpersistent disks**

Description

Reference value: **One of the following: * Not present (defaults to Persistent if blank) * Explicitly set to Persistent *Set to Independent-Persistent**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Hardware". Click "Edit". Expand "Hard disk", go to "Disk mode" and choose "Independent - Nonpersistent".

🟥	**Parameter**	Severity:	High

Title **Disable VIX messages from the VM**

Description

Reference value: **True**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.vixMessage.disable" parameter with the value "true".

🟥	**Parameter**	Severity:	High

Title **Disable tools auto install**

Description

Reference value: **True**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "isolation.tools.autoInstall.disable" parameter with the value "true".

🟥	**Parameter**	Severity:	High

Title **Limit informational messages from the VM to the VMX file**

Description

Reference value: **1048576**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "tools.setInfo.sizeLimit" parameter with the value "1048576".

Parameter Severity: High

Title **Control access to VM console via VNC protocol**

Description

Reference value: **FALSE**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "RemoteDisplay.vnc.enabled" parameter with the value "false".

Parameter Severity: High

Title **Do not send host information to guests**

Description

Reference value: **False**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "tools.guestlib.enableHostInfo" parameter with the value "false".

Parameter Severity: High

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

Description

Reference value: **Site-Specific**

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).

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then edit "sched.mem.pshare.salt" parameter with the value "Site-Specific".

Parameter Severity: High

Title **Control access to VMs through the dvfilter network APIs**

Description

Reference value: **Null unless using dvfilter**

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.

Remediation

From the VMware vSphere web client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "VM Options". Click "Edit". Go to "VM Options" tab and expand "Advanced". Click on "Edit Configuration". Click on "Add Row" and then add "ethernetn.filtern.name" parameter with the filtername value.

Parameter Severity: High

Title **Audit all uses of PCI or PCIe passthrough functionality**

Description

Reference value: **NULL**

Using the VMware DirectPath I/O feature to pass through a PCI or PCIe device to a virtual machine results in a potential security vulnerability. The vulnerability can be triggered by buggy or malicious code running in privileged mode in the guest OS, such as a device driver. Industry-standard hardware and firmware does not currently have sufficient error containment support to make it possible for ESXi to close the vulnerability fully. There can be a valid business reason for a VM to have this configured. This is an audit-only guideline. You should be aware of what virtual machines are configured with direct passthrough of PCI and PCIe devices and ensure that their guest OS is monitored carefully for malicious or buggy drivers that could crash the host.

Remediation

From the VMware vSphere Web Client, select each VM and click "Manage" ("Configure" in 6.5) -> "Settings" -> "Virtual Hardware" -> Remove the PCI/PCIe passthrough device.

Group

Title **vNetwork**

Description

Represents a network accessible by either hosts or virtual machines. This can be a physical network or a logical network, such as a VLAN.

If this section is not applicable than there is no switches.

Parameter Severity: High

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

Description

Reference value: **1**

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.

Remediation

From VMware vSphere Web cClient, select the host and then click "Manage" ("Configure" in 6.5) -> "Settings" -> "System" -> "Advanced System settings". Filter for Net.BlockGuestBPDU to see the configured value. Click edit and set it to the desired value.

Parameter Severity: High

Title

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

Description

Reference value: **Reject**

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.

Remediation

From the VMware vSphere Web Client select the host and click "Manage" ("Configure" in 6.5) -> "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".

Parameter Severity: High

Title

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

Description

Reference value: **Reject**

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.

Remediation

From the VMware vSphere web client select the host and click "Manage" ("Configure" in 6.5) -> "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".

Parameter Severity: High

Title

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

Description

Reference value: **Reject**

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.

Remediation

From the VMware vSphere Web Client select the host and click "Manage" ("Configure" in 6.5) -> "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".

Parameter	Severity: High
Title	**Prevent unintended use of dvfilter network APIs**

Description

Reference value: **Null**

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.

Remediation

From VMware vSphere web client, select host and then click "Manage" ("Configure" in 6.5) -> "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.

The end of the report. RedCheck 1.7.0.9.
RedCheckID: F783047D-DF52-4E7B-9576-E7299B4A35FF.