Security Hardening | HIPAA

Generated from Runecast Analyzer on Nov 6, 2018 at 08:09 PM, GMT (UTCZ)

vCenters [redacted]

Sorted by result (desc), severity (desc), ruleId (asc)

Table filters (none)

Severity	Title	Applies to	Products	Objects	Rule ID	Result	Note
Major	Ensure default setting for intra-VM TPS is correct: ESXi. TransparentPageSharing-intra-enabled (164.308 (a) (1) (ii) (B))	Compute	vSphere	1	164.308 (a) (1) (ii) (B)	Fail	
Major	Set the time after which a locked account is automatically unlocked: ESXi.set-account-auto-unlock-time (164.308 (a) (1) (ii) (B))	Compute	vSphere	2	164.308 (a) (1) (ii) (B)	Fail	
Major	Keep ESXi system properly patched: ESXi.apply-patches (164.308 (a) (5) (ii) (B))	Compute	vSphere	2	164.308 (a) (5) (ii) (B)	Fail	
Major	Establish a password policy for password complexity: ESXi.set-password-policies (164.308 (a) (5) (ii) (D))	Compute	vSphere	2	164.308 (a) (5) (ii) (D)	Fail	
Major	Set the count of maximum failed login attempts before the account is locked out: ESXi.set-account-lockout (164.308 (a) (5) (ii) (D))	Compute	vSphere	2	164.308 (a) (5) (ii) (D)	Fail	
Major	Enable lockdown mode to restrict remote access: enable-lockdown-mode (164.312 (a) (1))	Compute	vSphere	2	164.312 (a) (1)	Fail	
Major	Set DCUI.Access to allow trusted users to override lockdown mode: set-dcui-access (164.312 (a) (1))	Compute	vSphere	2	164.312 (a) (1)	Fail	
Major	Use Active Directory for local user authentication: enable-ad-auth (164.312 (a) (2) (i))	Compute	vSphere	2	164.312 (a) (2) (i)	Fail	
Major	Check vCenter has syslogging enabled (164.312 (b))	Manage	vSphere	1	164.312 (b)	Fail	

Major	**Configure remote logging for ESXi hosts: enable-remote-syslog (164.312 (b))**	**Compute**	**vSphere**	**2**	**164.312 (b)**	**Fail**	
Major	**Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled: enable-bpdu-filter (164.312 (e) (1))**	**Network**	**vSphere**	**2**	**164.312 (e) (1)**	**Fail**	
Major	**Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit (164.312 (e) (1))**	**Network**	**vSphere**	**2**	**164.312 (e) (1)**	**Fail**	
Major	**Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit-dvportgroup (164.312 (e) (1))**	**Network**	**vSphere**	**7**	**164.312 (e) (1)**	**Fail**	
Major	**Ensure that the MAC Address Change policy is set to reject: reject-mac-change-dvportgroup (164.312 (e) (1))**	**Network**	**vSphere**	**7**	**164.312 (e) (1)**	**Fail**	
Major	**Ensure that the MAC Address Change policy is set to reject: reject-mac-changes (164.312 (e) (1))**	**Network**	**vSphere**	**2**	**164.312 (e) (1)**	**Fail**	
Major	**Ensure that the Promiscuous Mode policy is set to reject: reject-promiscuous-mode-dvportgroup (164.312 (e) (1))**	**Network**	**vSphere**	**4**	**164.312 (e) (1)**	**Fail**	
Major	**Restrict port-level configuration overrides on VDS : vNetwork. restrict-port-level-overrides (164.312 (e) (1))**	**Network**	**vSphere**	**7**	**164.312 (e) (1)**	**Fail**	
Medium	**Avoid using independent nonpersistent disks: disable-independent-nonpersistent (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**2**	**164.308 (a) (1) (ii) (B)**	**Fail**	
Medium	**Disable tools auto install: disable-autoinstall (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**76**	**164.308 (a) (1) (ii) (B)**	**Fail**	
Medium	**Disable virtual disk shrinking: disable-disk-shrinking-shrink (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**67**	**164.308 (a) (1) (ii) (B)**	**Fail**	
Medium	**Disable virtual disk shrinking: disable-disk-shrinking-wiper (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**67**	**164.308 (a) (1) (ii) (B)**	**Fail**	
Medium	**Disconnect unauthorized devices: disconnect-devices-floppy (164. 308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**30**	**164.308 (a) (1) (ii) (B)**	**Fail**	
Medium	**Do not send host information to guests: restrict-host-info (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**77**	**164.308 (a) (1) (ii) (B)**	**Fail**	

Medium	Explicitly disable copy/paste operations: disable-console-copy (164.308 (a) (1) (ii) (B))	VM	vSphere	67	164.308 (a) (1) (ii) (B)	Fail	
Medium	Explicitly disable copy/paste operations: disable-console-dnd (164.308 (a) (1) (ii) (B))	VM	vSphere	67	164.308 (a) (1) (ii) (B)	Fail	
Medium	Explicitly disable copy/paste operations: disable-console-gui-options (164.308 (a) (1) (ii) (B))	VM	vSphere	67	164.308 (a) (1) (ii) (B)	Fail	
Medium	Explicitly disable copy/paste operations: disable-console-paste (164.308 (a) (1) (ii) (B))	VM	vSphere	67	164.308 (a) (1) (ii) (B)	Fail	
Medium	Limit informational messages from the VM to the VMX file: limit-setinfo-size (164.308 (a) (1) (ii) (B))	VM	vSphere	68	164.308 (a) (1) (ii) (B)	Fail	
Medium	Prevent unauthorized removal, connection and modification of devices: prevent-device-interaction-connect (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Medium	Prevent unauthorized removal, connection and modification of devices: prevent-device-interaction-edit (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Medium	Control access to VM console via VNC protocol: minimize-console-VNC-use (164.312 (a) (1))	VM	vSphere	77	164.312 (a) (1)	Fail	
Medium	The system must configure the firewall to restrict access to services running on the host (164.312 (e) (1))	Compute	vSphere	2	164.312 (e) (1)	Fail	
Low	Disable HGFS file transfers: disable-hgfs (164.308 (a) (1) (ii) (B))	VM	vSphere	77	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable VIX messages from the VM: disable-vix-messages (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-autologon (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-biosbbs (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-getcreds (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	

Low	Disable certain unexposed features: disable-unexposed-features-launchmenu (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-memsfss (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-protocolhandler (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-shellaction (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-toporequest (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-trashfolderstate (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-trayicon (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unity (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unity-interlock (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unity-taskbar (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unity-unityactive (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unity-windowcontents (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-unitypush (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	Disable certain unexposed features: disable-unexposed-features-versionget (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	

Low	Disable certain unexposed features: disable-unexposed-features-versionset (164.308 (a) (1) (ii) (B))	VM	vSphere	76	164.308 (a) (1) (ii) (B)	Fail	
Low	The system must disable Inter-VM transparent page sharing (164.308 (a) (1) (ii) (B))	Compute	vSphere	1	164.308 (a) (1) (ii) (B)	Fail	
Low	Enable Strict lockdown mode to restrict access: ESXi.enable-strict-lockdown-mode (164.312 (a) (1))	Compute	vSphere	2	164.312 (a) (1)	Fail	
Low	The system must use Active Directory for local user authentication (164.312 (a) (2) (i))	Compute	vSphere	2	164.312 (a) (2) (i)	Fail	
Low	VM is configured to forward logs to syslog server (164.312 (b))	VM	vSphere	75	164.312 (b)	Fail	
Major	Configure NTP time synchronization: config-ntp (164.308 (a) (1) (ii) (B))	Compute	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Major	Disable TLS 1.0 and 1.1 on ESXi Hosts if necessary: ESXi.Disable-oldtls-protocols (164.308 (a) (1) (ii) (B))	Compute	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Major	Enable bidirectional CHAP, also known as Mutual CHAP, authentication for iSCSI traffic: enable-chap-auth (164.308 (a) (1) (ii) (B))	Compute	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Major	NTP Server not running in ESX (164.308 (a) (1) (ii) (B))	Compute	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Major	Prevent unintended use of dvfilter network APIs: verify-dvfilter-bind (164.308 (a) (1) (ii) (B))	Compute	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Major	Verify Image Profile and VIB Acceptance Levels: ESXi.verify-acceptance-level-supported (164.308 (a) (5) (ii) (B))	Compute	vSphere	0	164.308 (a) (5) (ii) (B)	Configured	
Major	Ensure that vpxuser auto-password change meets policy: vpxuser-password-age (164.308 (a) (5) (ii) (D))	vCenter	vSphere	0	164.308 (a) (5) (ii) (D)	Configured	
Major	Passwords for ESXi hosts require a minimum of 7 characters. (164.308 (a) (5) (ii) (D))	Compute	vSphere	0	164.308 (a) (5) (ii) (D)	Configured	
Major	Disable ESXi Shell unless needed for diagnostics or troubleshooting: disable-esxi-shell (164.312 (a) (1))	Compute	vSphere	0	164.312 (a) (1)	Configured	

Major	**Disable Managed Object Browser (MOB): ESXi.disable-mob (164.312 (a) (1))**	**Compute**	**vSphere**	**0**	**164.312 (a) (1)**	**Configured**	
Major	**Disable SSH: disable-ssh (164.312 (a) (1))**	**Compute**	**vSphere**	**0**	**164.312 (a) (1)**	**Configured**	
Major	**The SSH daemon must be configured to use only the SSHv2 protocol (164.312 (a) (1))**	**Compute**	**vSphere**	**0**	**164.312 (a) (1)**	**Configured**	
Major	**For ESXi host, default root user account has been disabled so that it has NoAccess priveleges (164.312 (a) (2) (i))**	**Compute**	**vSphere**	**0**	**164.312 (a) (2) (i)**	**Configured**	
Major	**Audit DCUI timeout value: ESXi.set-dcui-timeout (164.312 (a) (2) (iii))**	**Compute**	**vSphere**	**0**	**164.312 (a) (2) (iii)**	**Configured**	
Major	**Set a timeout to automatically terminate idle ESXi Shell and SSH sessions: set-shell-interactive-timeout (164.312 (a) (2) (iii))**	**Compute**	**vSphere**	**0**	**164.312 (a) (2) (iii)**	**Configured**	
Major	**Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run: set-shell-timeout (164.312 (a) (2) (iii))**	**Compute**	**vSphere**	**0**	**164.312 (a) (2) (iii)**	**Configured**	
Major	**Configure persistent logging for all ESXi host: ESXi.config-persistent-logs (164.312 (b))**	**Compute**	**vSphere**	**0**	**164.312 (b)**	**Configured**	
Major	**Disable VDS network healthcheck if you are not actively using it: limit-network-healthcheck (164.312 (e) (1))**	**Network**	**vSphere**	**0**	**164.312 (e) (1)**	**Configured**	
Major	**Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT): no-vgt-vlan-4095 (164.312 (e) (1))**	**Network**	**vSphere**	**0**	**164.312 (e) (1)**	**Configured**	
Major	**Ensure that the Promiscuous Mode policy is set to reject: reject-promiscuous-mode (164.312 (e) (1))**	**Network**	**vSphere**	**0**	**164.312 (e) (1)**	**Configured**	
Major	**Ensure the the ESXi host firewall is enabled (164.312 (e) (1))**	**Network**	**vSphere**	**0**	**164.312 (e) (1)**	**Configured**	
Medium	**Audit all uses of PCI or PCIe passthrough functionality: verify-PCI-Passthrough (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	
Medium	**Control access to VMs through VMsafe CPU/memory APIs: verify-vmsafe-cpumem-agentaddress (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	
Medium	**Control access to VMs through VMsafe CPU/memory APIs: verify-vmsafe-cpumem-agentport (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	

Medium	Control access to VMs through VMsafe CPU/memory APIs: verify-vmsafe-cpumem-enable (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disable 3D features on Server and desktop virtual machines: disable-non-essential-3D-features (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disable VM-to-VM communication through VMCI: disable-intervm-vmci (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disable all but VGA mode on virtual machines: enable-VGA-Only-Mode (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disconnect unauthorized devices: disconnect-devices-ide (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disconnect unauthorized devices: disconnect-devices-parallel (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disconnect unauthorized devices: disconnect-devices-serial (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Disconnect unauthorized devices: disconnect-devices-usb (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Limit VM logging: limit-log-number (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Limit VM logging: limit-log-size (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Limit sharing of console connections: limit-console-connections-one (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Prevent virtual machines from taking over resources: control-resource-usage (164.308 (a) (1) (ii) (B))	VM	vSphere	0	164.308 (a) (1) (ii) (B)	Configured	
Medium	Control access to VMs through the dvfilter network APIs: verify-network-filter (164.312 (a) (1))	VM	vSphere	0	164.312 (a) (1)	Configured	
Medium	Ensure SSL for Network File copy (NFC) is enabled: verify-nfc-ssl (164.312 (e) (1))	vCenter	vSphere	0	164.312 (e) (1)	Configured	
Medium	The system must configure the firewall to block network traffic by default (164.312 (e) (1))	Compute	vSphere	0	164.312 (e) (1)	Configured	

Medium	**Verify that the autoexpand option for VDS dvPortgroups is disabled: disable-dvportgroup-autoexpand (164.312 (e) (1))**	**Network**	**vSphere**	**0**	**164.312 (e) (1)**	**Configured**	
Low	**Disable VM Monitor Control: disable-monitor-control (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	
Low	**Disable VM logging: disable-logging (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	
Low	**Limit sharing of console connections: limit-console-connections-two (164.308 (a) (1) (ii) (B))**	**VM**	**vSphere**	**0**	**164.308 (a) (1) (ii) (B)**	**Configured**	
Low	**Disable DCUI to prevent local administrative control: disable-dcui (164.312 (a) (1))**	**Compute**	**vSphere**	**0**	**164.312 (a) (1)**	**Configured**	