Runecast

November 7, 2018 by Runecast Analyzer

Overall System Health

Configuration Issues by Severity

Critical 7

Major 32

Medium 21

Low 29

Log Issues

Enable collection of logs to see real-time actionable insights into your environment.

Security Compliance

42%

KBs Applicable

21

Best Practice Adoption

58%

Configuration Issues by Layer

Management (4)

2 | 2

VM (54)

1 | 7 | 20 | 26

Compute (20)

4 | 15 | 1

Network (9)

9

Storage (2)

1 | 1

Issue History

Issue history will become available when an analysis has been performed during a previous day.

Hosts with Most Issues

[redacted] 3 | 25 | 17 | 25

[redacted] 2 | 22 | 15 | 24

Analysis Detail ([redacted])

November 7, 2018 1:19 AM

Total Checks Performed:	KB Checks:	Security Hardening Checks:	Best Practice Checks:
37,275	29,477	6,785	1,013

Analyzed objects

Clusters:	2	Folders:	27
Datacenters:	1	Hosts:	2
Datastores:	6	Networks:	5
Datastore clusters:	1	Resource pools:	6
dvPortgroups:	7	vApps:	3
dvSwitches:	2	VMs:	75

Top 50 Issues

Severity	Issue Title	Source	Applies To	Affects	Products	Objects
Critical	Hypervisor-Assisted Guest Mitigation for Branch Target injection (52085)	Knowledge Base	vCenter	Security	vSphere	45
Critical	VMware Security Advisory: VMSA-2018-0017.4 (VMware Tools update addresses an out-of-bounds read vulnerability)	Knowledge Base	VM	Security	vSphere	20
Critical	VMware ESXi 5.5 & 6.0 fail with PSOD when IPFIX is disabled (2149909)	Knowledge Base	Compute	Availability	vSphere	4
Critical	ESXi host fails with purple screen error: "NOT_IMPLEMENTED bora/vmkernel/filesystems/devfs/devfs.c:2655" (2150280)	Knowledge Base	Compute	Availability	vSphere	2
Critical	Disable SSH unless needed for diagnostics or troubleshooting	Best Practices	Compute	Security	vSphere	1
Critical	VMware Security Advisory: VMSA-2018-00012.1 (Speculative Store Bypass issue)	Knowledge Base	Compute	Security	vSphere	1
Critical	VMware Security Advisory: VMSA-2018-0004 (Speculative execution issue, known as Spectre)	Knowledge Base	vCenter	Security	vSphere	1
Major	Virtual machine with multiple user login session fails with the error: GuestRpc: Channel X, conflict: guest application toolbox-dnd tried to register, but it is still registered on channel Y (2078823)	Knowledge Base	VM	Availability	vSphere	77
Major	Disabling the HotAdd/HotPlug capability in ESXi 6.x, 5.x and ESXi/ESX 4.x virtual machines (1012225)	Knowledge Base	VM	Availability	vSphere	76
Major	Allow only one remote console session at a time	Best Practices	VM	Security	vSphere	74
Major	ESXi hostd service might stop responding when there is an IO failure on the storage side (2149947)	Knowledge Base	Compute	Manageability	vSphere	41
Major	"vami.netmask0.vm-name. Network has no associated network protocol profile" when powering on the virtual machine (2070950)	Knowledge Base	VM	Availability	vSphere	26
Major	Ensure that the Forged Transmits policy is set to Reject	Best Practices	Network	Security	vSphere	8
Major	Ensure that the MAC Address Change policy is set to Reject	Best Practices	Network	Security	vSphere	8
Major	Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit-dvportgroup	VMware Security Hardening	Network	Security	vSphere	7
Major	Ensure that the MAC Address Change policy is set to reject: reject-mac-change-dvportgroup	VMware Security Hardening	Network	Security	vSphere	7
Major	Restrict port-level configuration overrides on VDS : vNetwork.restrict-port-level-overrides	VMware Security Hardening	Network	Security	vSphere	7
Major	Ensure that the Promiscuous Mode policy is set to	VMware	Network	Security	vSphere	4

Severity	Issue Title	Source	Applies To	Affects	Products	Objects
	reject: reject-promiscuous-mode-dvportgroup	Security Hardening				
Major	Ensure more than 15% free space on a datatore	Best Practices	Storage	Manageability	vSphere	3
Major	Virtual machine cannot boot when controller type for the operating system and data drive is Paravirtualized SCSI (1023592)	Knowledge Base	VM	Availability	vSphere	3
Major	Ensure redundancy for each portgroup	Best Practices	Compute	Availability	vSphere	2
Major	Set timeouts for ESXi Shell and SSH sessions	Best Practices	Compute	Security	vSphere	2
Major	Advanced setting "ScratchConfig.ConfiguredScratchLocation" for persistent scratch location is reverted to the default value after ESXi 6.x host reboot (2151270)	Knowledge Base	Compute	Security	vSphere	2
Major	Powering on the virtual machine fails with the error: Thin/TBZ disks cannot be opened in multiwriter mode (1033570)	Knowledge Base	VM	Availability	vSphere	2
Major	Configure remote logging for ESXi hosts: enable-remote-syslog	VMware Security Hardening	Compute	Security	vSphere	2
Major	Configure the ESXi host firewall to restrict access to services running on the host	VMware Security Hardening	Compute	Security	vSphere	2
Major	Enable lockdown mode to restrict remote access: enable-lockdown-mode	VMware Security Hardening	Compute	Security	vSphere	2
Major	Establish a password policy for password complexity: ESXi.set-password-policies	VMware Security Hardening	Compute	Security	vSphere	2
Major	Keep ESXi system properly patched: ESXi.apply-patches	VMware Security Hardening	Compute	Security	vSphere	2
Major	Set DCUI.Access to allow trusted users to override lockdown mode: set-dcui-access	VMware Security Hardening	Compute	Security	vSphere	2
Major	Set the count of maximum failed login attempts before the account is locked out: ESXi.set-account-lockout	VMware Security Hardening	Compute	Security	vSphere	2
Major	Set the time after which a locked account is automatically unlocked: ESXi.set-account-auto-unlock-time	VMware Security Hardening	Compute	Security	vSphere	2
Major	Use Active Directory for local user authentication: enable-ad-auth	VMware Security Hardening	Compute	Security	vSphere	2
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	VMware Security Hardening	Network	Security	vSphere	2
Major	Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit	VMware Security	Network	Security	vSphere	2

Severity	Issue Title	Source	Applies To	Affects	Products	Objects
		Hardening				
Major	Ensure that the MAC Address Change policy is set to reject: reject-mac-changes	VMware Security Hardening	Network	Security	vSphere	2
Major	Set alternate isolation address for HA cluster	Best Practices	Compute	Availability	vSphere	1
Major	Enable Strict Admission Control in a cluster	Best Practices	VM	Recoverability	vSphere	1
Major	Ensure default setting for intra-VM TPS is correct: ESXi.TransparentPageSharing-intra-enabled	VMware Security Hardening	Compute	Security	vSphere	1
Medium	Control access to VM console via VNC protocol: minimize-console-VNC-use	VMware Security Hardening	VM	Security	vSphere	77
Medium	Do not send host information to guests: restrict-host-info	VMware Security Hardening	VM	Security	vSphere	77
Medium	Disable tools auto install: disable-autoinstall	VMware Security Hardening	VM	Security	vSphere	76
Medium	Prevent unauthorized removal, connection and modification of devices: prevent-device-interaction-connect	VMware Security Hardening	VM	Security	vSphere	76
Medium	Prevent unauthorized removal, connection and modification of devices: prevent-device-interaction-edit	VMware Security Hardening	VM	Security	vSphere	76
Medium	Limit informational messages from the VM to the VMX file: limit-setinfo-size	VMware Security Hardening	VM	Security	vSphere	68
Medium	Disable virtual disk shrinking: disable-disk-shrinking-shrink	VMware Security Hardening	VM	Security	vSphere	67
Medium	Disable virtual disk shrinking: disable-disk-shrinking-wiper	VMware Security Hardening	VM	Security	vSphere	67
Medium	Explicitly disable copy/paste operations: disable-console-copy	VMware Security Hardening	VM	Security	vSphere	67
Medium	Explicitly disable copy/paste operations: disable-console-dnd	VMware Security Hardening	VM	Security	vSphere	67
Medium	Explicitly disable copy/paste operations: disable-console-gui-options	VMware Security Hardening	VM	Security	vSphere	67