tenable
network security

Addressing the Security Challenges of Virtualization

“Vulnerabilities Exposed” Webcast Series Part 2

Paul Asadoorian, Jack Daniel,
& Russell Butturini

“Vulnerabilities Exposed” Series

- Part **2** of a 4-part series
- Part 1: “Reducing Your Patch Cycle to Less Than 5 Days” is available
- Archives & slides: www.tenable.com/vulns-exposed

Strategies & solutions for today’s common security challenges

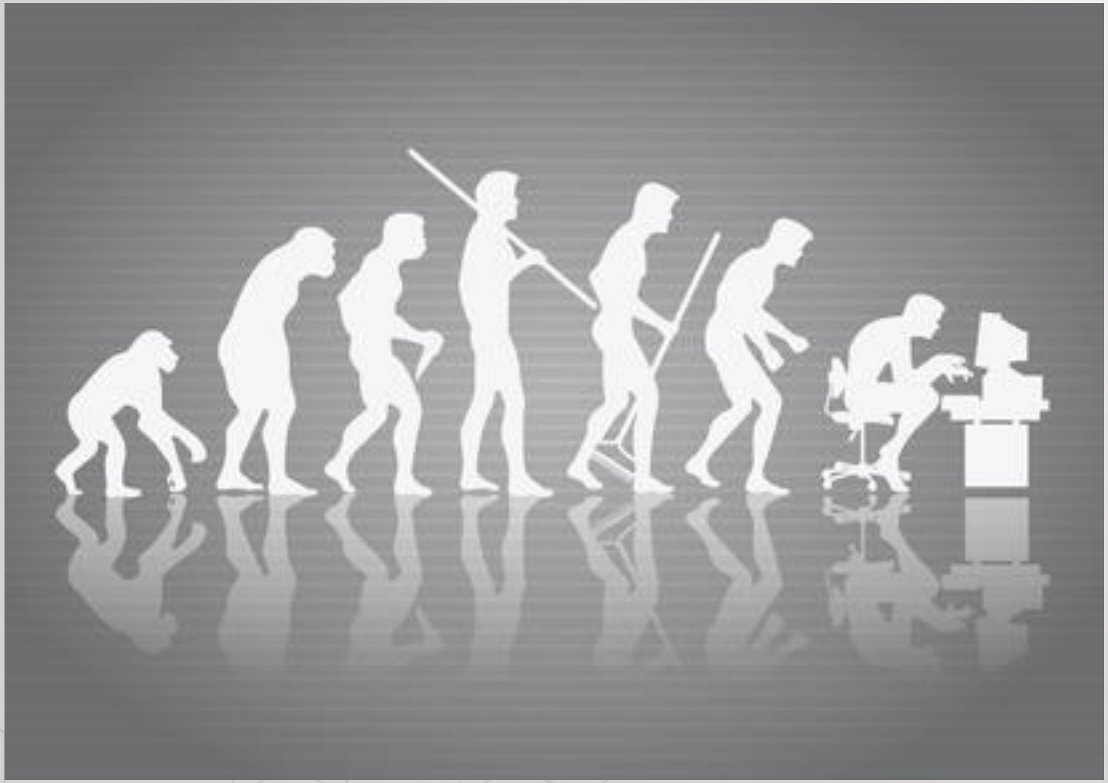
tenable
network security

Today’s Webcast Roadmap

- Virtualization evolution – How we got here
- Virtualization challenges – The problems we face
- Solutions – Procedural & tactical

tenable
network security

Virtualization Evolution



In the Beginning, There Was One

Source: ibm.com

IBM System/370: supported virtual memory & virtual disks

Ran multiple OSes at once

Took up LOTS of space!

Then There Were Many

LOTS of servers!

Ran one OS at a time

Cables, heat, noise, & power consumption

Source: futurepredictions.com

And Now…

Source: dell.com

Back to one big server!

Runs multiple OSes at once!

Virtual memory & virtual disks!

Difference: Takes up way less space, consumes less power, less wiring, & generates slightly less heat

Virtualization Problems

Having your own cloud is not all it’s cracked up to be…

Problem: “VM Sprawl”

- Easy to create & clone servers
- Disk space & memory costs falling
- Allows you to scratch itch for new servers

End result: Greatly increased attack surface!

Problem: “Whack-a-Mole”

- VMs easy to create then suspend
- What happens when someone else brings it online 3 months later?
- Is it up-to-date on patches and hardened?
- Creates several moving targets…

End result: Your attack surface is ever-changing!

Virtualization Abstracts the Physical Layer

- Successful virtualization layer attacks put attacker in your datacenter
- Guest OSes can be attacked to jump into host virtualization
  - Even if your guest OS is fully patched & hardened

End result: Successful attacks against virtualization layer will obtain access to all hosted servers

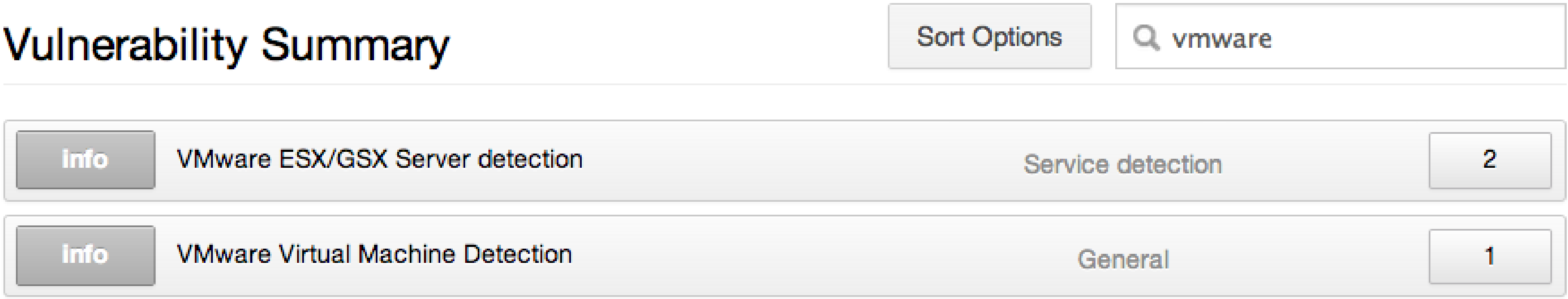
Solution: Nessus

Photo Credit: www.thinkgeek.com

Nessus is your Ninja Umbrella!

Nessus Discovers VMware

You don’t know what you don’t know (until you run a Nessus scan)



Vulnerability Summary

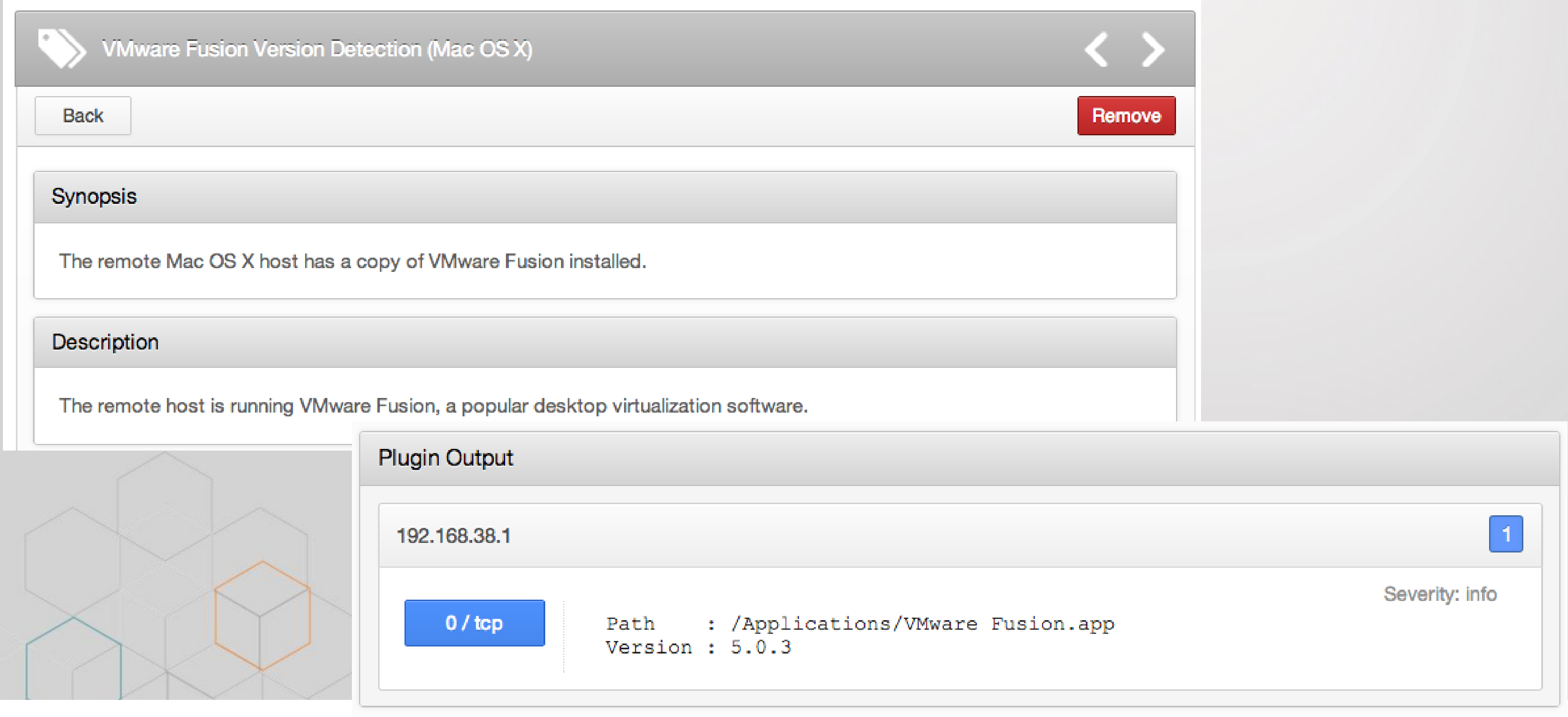
Info	VMware ESX/GSX Server detection	Service detection	2
Info	VMware Virtual Machine Detection	General	1

No credentials required

tenable
network security

VMware Discovery: Workstations

Discovers VMware clients, such as VMware workstation & VMware Fusion



Synopsis

The remote Mac OS X host has a copy of VMware Fusion installed.

Description

The remote host is running VMware Fusion, a popular desktop virtualization software.

Plugin Output

192.168.38.1 1

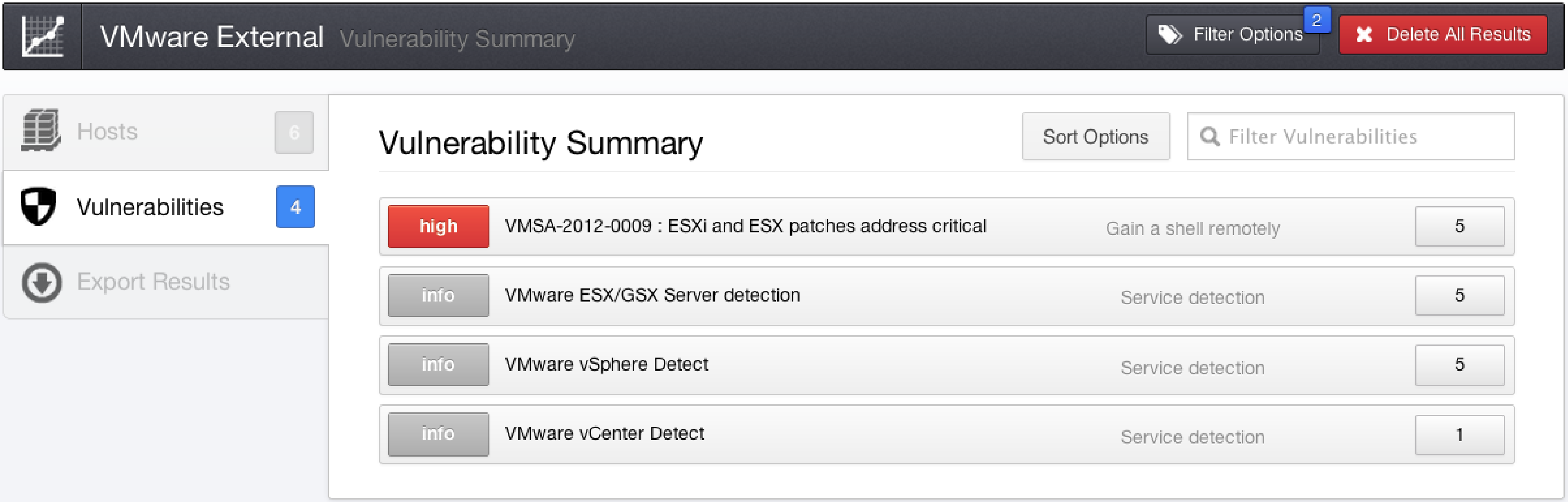
Severity: info

0 / tcp

```
Path    : /Applications/VMware Fusion.app
Version : 5.0.3
```

VMware Local Patch Checking

Supports VMware Fusion, Workstation, vSphere, & vCenter

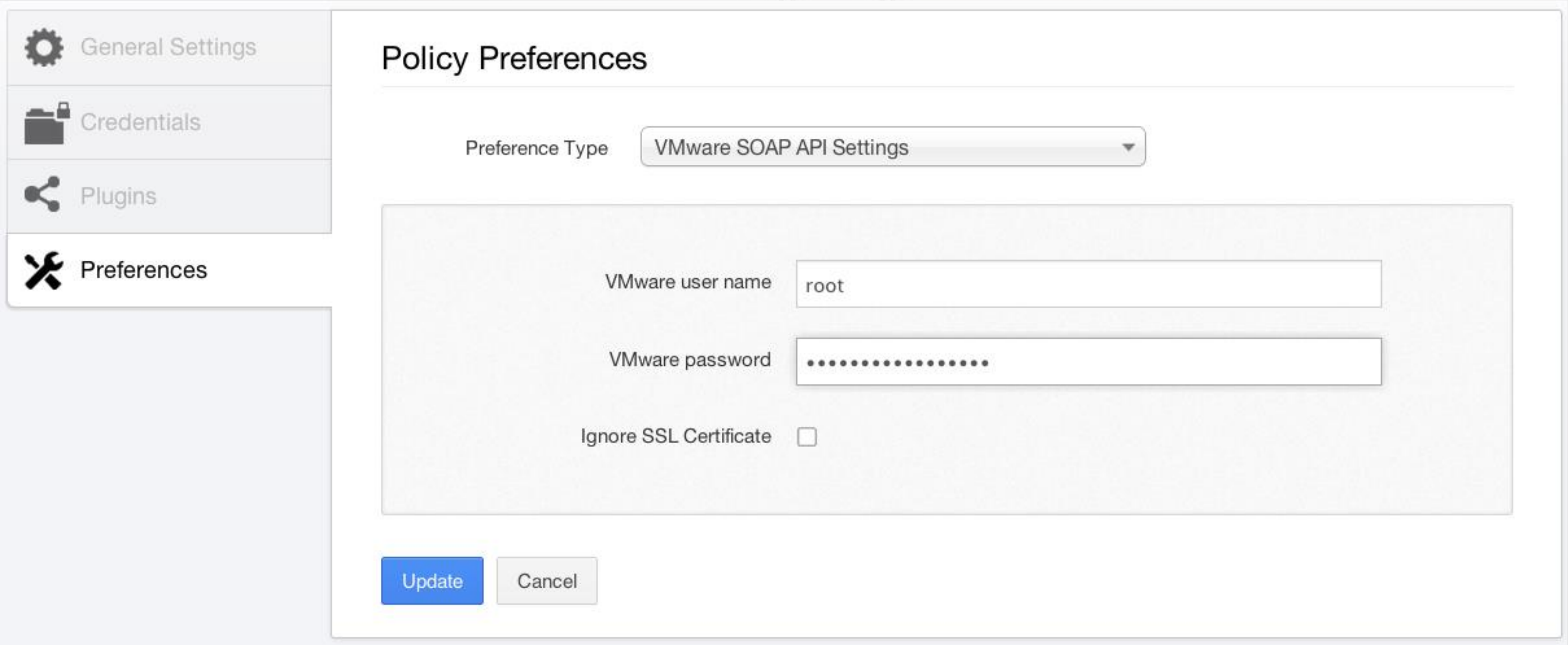


Vulnerability Summary

high	VMSA-2012-0009 : ESXi and ESX patches address critical	Gain a shell remotely	5
info	VMware ESX/GSX Server detection	Service detection	5
info	VMware vSphere Detect	Service detection	5
info	VMware vCenter Detect	Service detection	1

tenable network security

Secure Access to VMware API



Policy Preferences

Preference Type: VMware SOAP API Settings

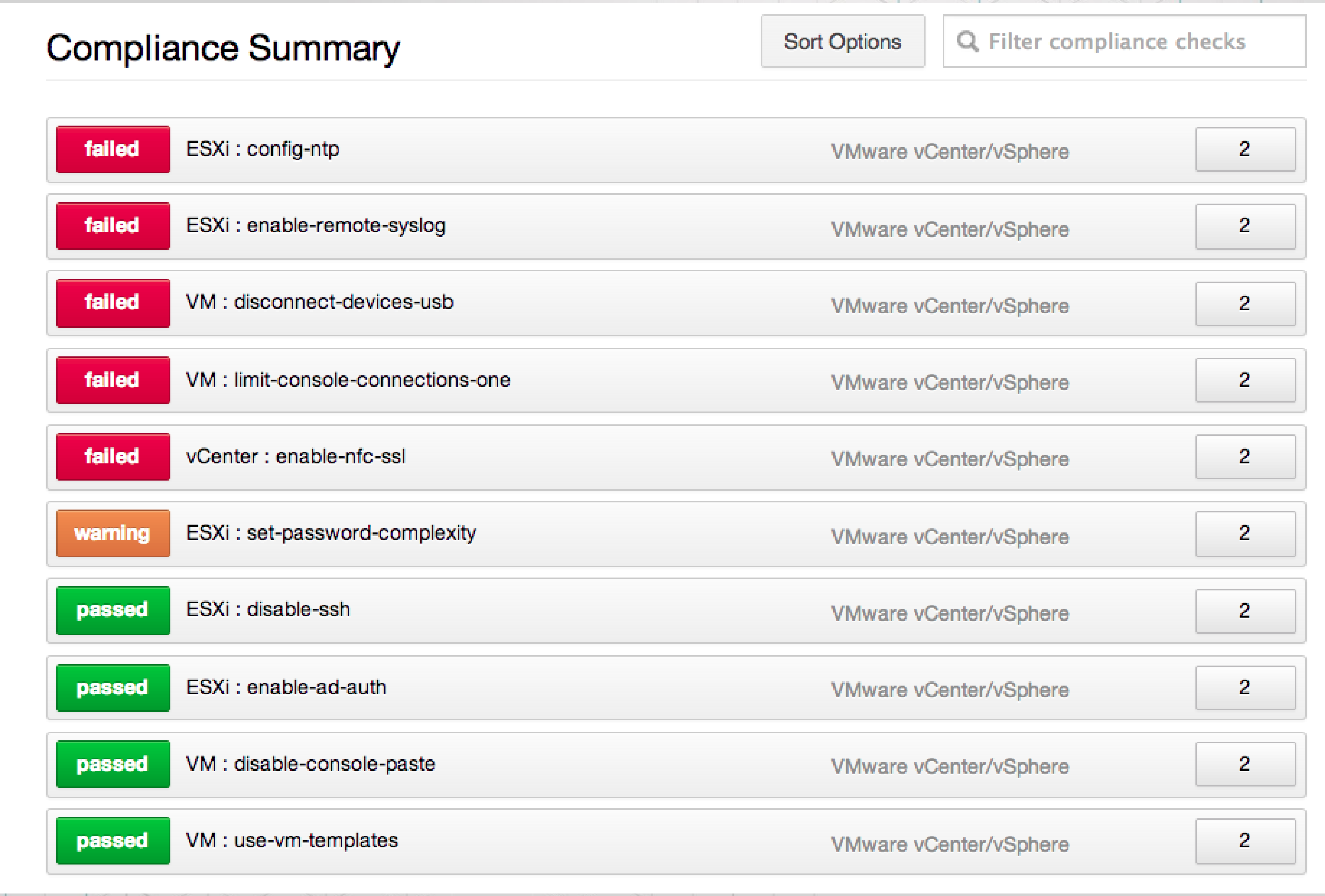
VMware user name: root

VMware password: ••••••••••••••••••

Ignore SSL Certificate ☐

VMware Configuration Auditing

- Compare your configuration
  - VMware's security guide
  - Tenable’s best practice guide
- Tune policies & compare against your production standards
- In-depth info examples:
  - VMware Tools installation status
  - OS info
  - Run state (active or suspended)

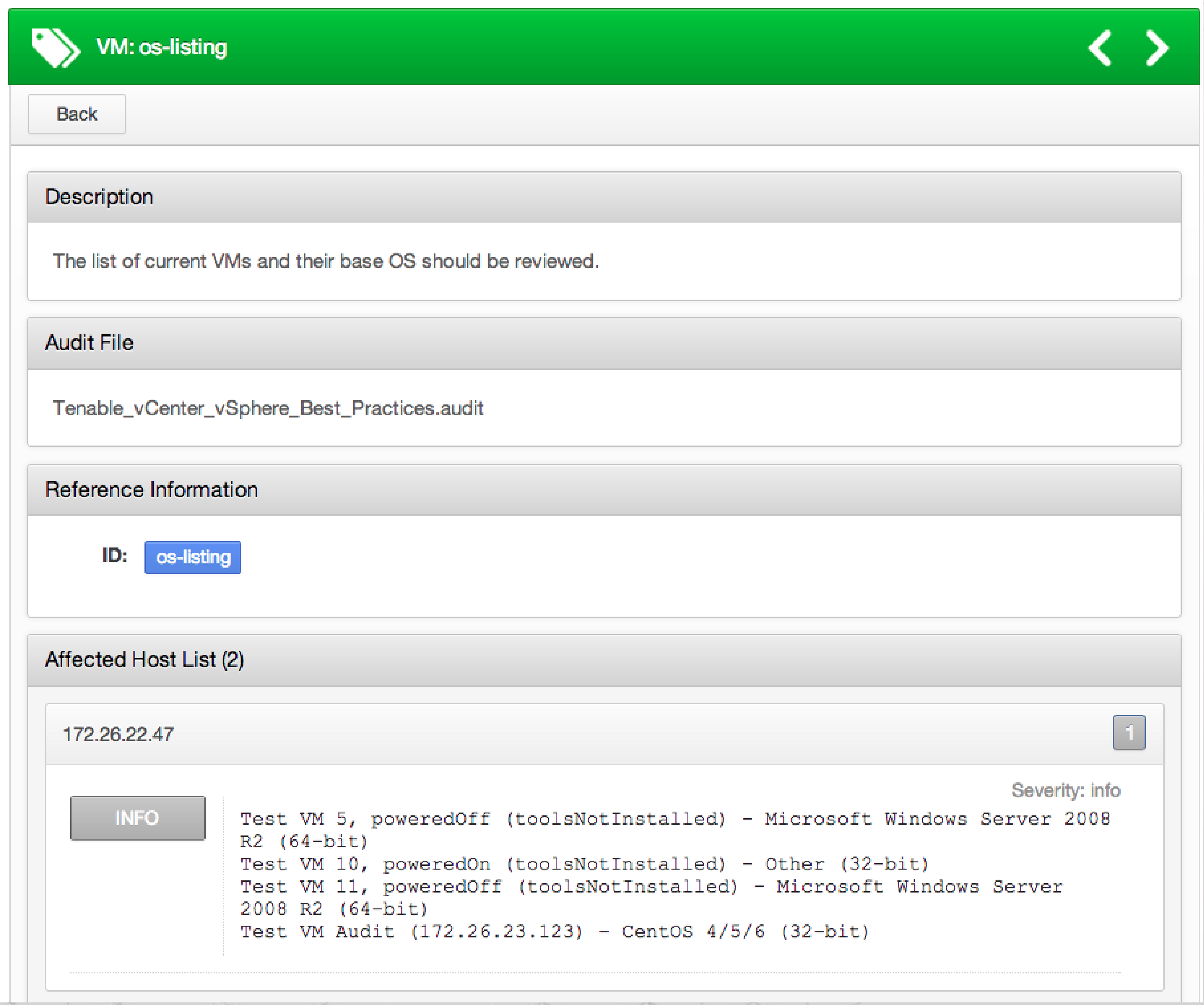


Compliance Summary

failed	ESXi : config-ntp	VMware vCenter/vSphere	2
failed	ESXi : enable-remote-syslog	VMware vCenter/vSphere	2
failed	VM : disconnect-devices-usb	VMware vCenter/vSphere	2
failed	VM : limit-console-connections-one	VMware vCenter/vSphere	2
failed	vCenter : enable-nfc-ssl	VMware vCenter/vSphere	2
warning	ESXi : set-password-complexity	VMware vCenter/vSphere	2
passed	ESXi : disable-ssh	VMware vCenter/vSphere	2
passed	ESXi : enable-ad-auth	VMware vCenter/vSphere	2
passed	VM : disable-console-paste	VMware vCenter/vSphere	2
passed	VM : use-vm-templates	VMware vCenter/vSphere	2

tenable
network security

VMware Virtual Machine Info



VM: os-listing

Description

The list of current VMs and their base OS should be reviewed.

Audit File

Tenable_vCenter_vSphere_Best_Practices.audit

Reference Information

ID: os-listing

Affected Host List (2)

172.26.22.47

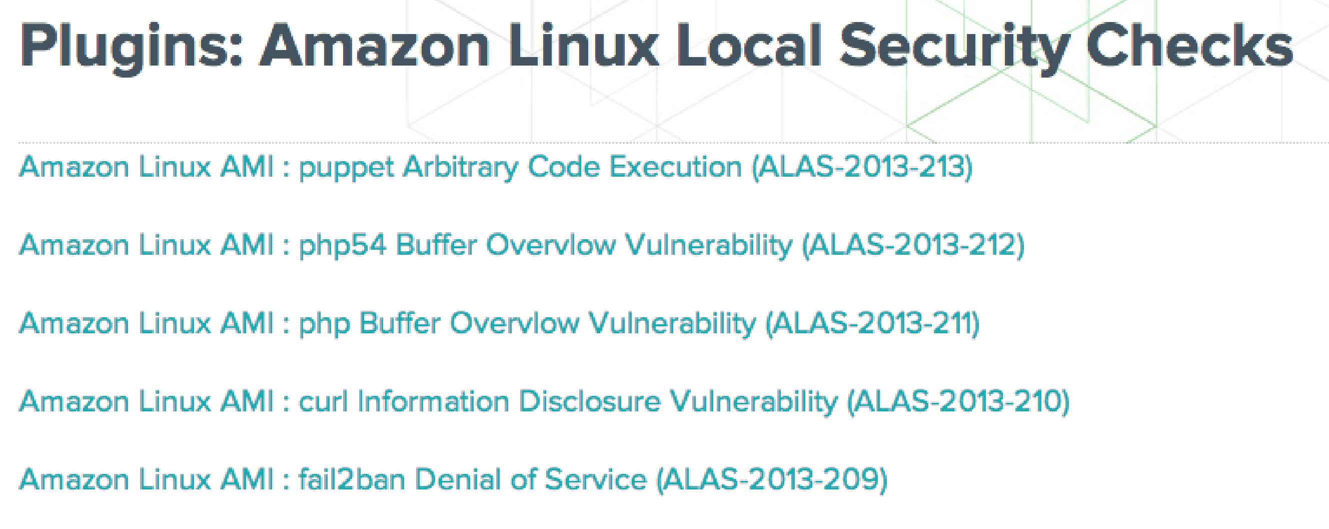
Severity: info

```
Test VM 5, poweredOff (toolsNotInstalled) - Microsoft Windows Server 2008
R2 (64-bit)
Test VM 10, poweredOn (toolsNotInstalled) - Other (32-bit)
Test VM 11, poweredOff (toolsNotInstalled) - Microsoft Windows Server
2008 R2 (64-bit)
Test VM Audit (172.26.23.123) - CentOS 4/5/6 (32-bit)
```

Amazon AMI Patch Checking

I get to say, *“Secure your cloud!”*

Make sure your Amazon AMI images are patched



Plugins: Amazon Linux Local Security Checks

Amazon Linux AMI : puppet Arbitrary Code Execution (ALAS-2013-213)

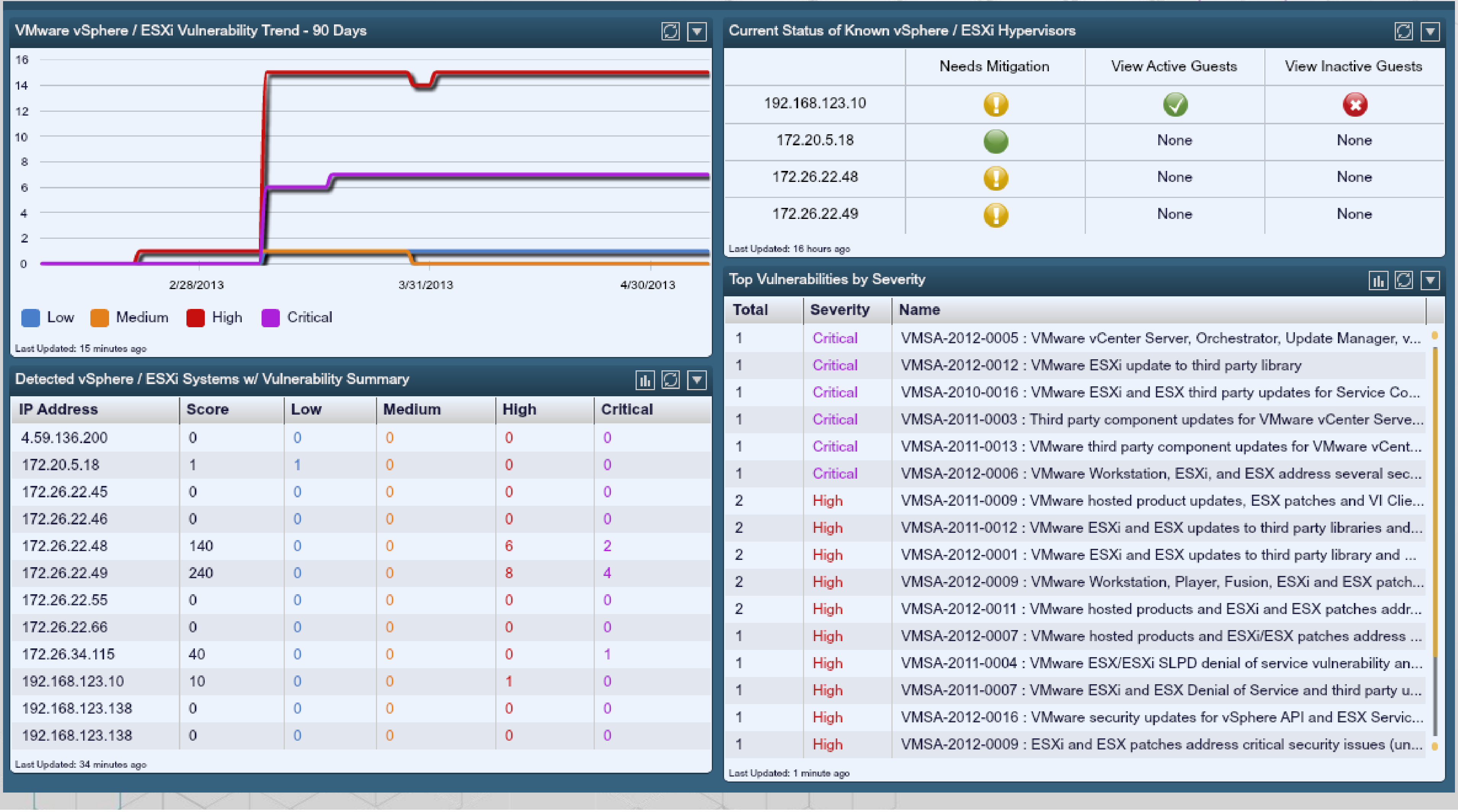
Amazon Linux AMI : php54 Buffer Overvlow Vulnerability (ALAS-2013-212)

Amazon Linux AMI : php Buffer Overvlow Vulnerability (ALAS-2013-211)

Amazon Linux AMI : curl Information Disclosure Vulnerability (ALAS-2013-210)

Amazon Linux AMI : fail2ban Denial of Service (ALAS-2013-209)

Solutions: SecurityCenter



VMware vSphere / ESXi Vulnerability Trend - 90 Days

Last Updated: 15 minutes ago

Detected vSphere / ESXi Systems w/ Vulnerability Summary

IP Address	Score	Low	Medium	High	Critical
4.59.136.200	0	0	0	0	0
172.20.5.18	1	1	0	0	0
172.26.22.45	0	0	0	0	0
172.26.22.46	0	0	0	0	0
172.26.22.48	140	0	0	6	2
172.26.22.49	240	0	0	8	4
172.26.22.55	0	0	0	0	0
172.26.22.66	0	0	0	0	0
172.26.34.115	40	0	0	0	1
192.168.123.10	10	0	0	1	0
192.168.123.138	0	0	0	0	0
192.168.123.138	0	0	0	0	0

Last Updated: 34 minutes ago

Current Status of Known vSphere / ESXi Hypervisors

	Needs Mitigation	View Active Guests	View Inactive Guests
192.168.123.10	!	✓	✗
172.20.5.18	●	None	None
172.26.22.48	!	None	None
172.26.22.49	!	None	None

Last Updated: 16 hours ago

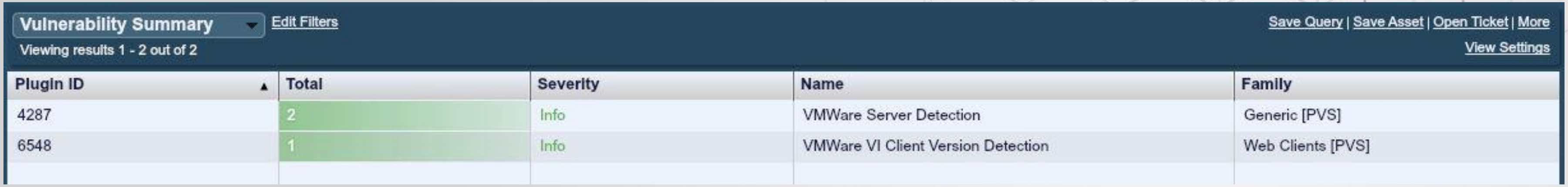
Top Vulnerabilities by Severity

Total	Severity	Name
1	Critical	VMSA-2012-0005 : VMware vCenter Server, Orchestrator, Update Manager, v...
1	Critical	VMSA-2012-0012 : VMware ESXi update to third party library
1	Critical	VMSA-2010-0016 : VMware ESXi and ESX third party updates for Service Co...
1	Critical	VMSA-2011-0003 : Third party component updates for VMware vCenter Serve...
1	Critical	VMSA-2011-0013 : VMware third party component updates for VMware vCent...
1	Critical	VMSA-2012-0006 : VMware Workstation, ESXi, and ESX address several sec...
2	High	VMSA-2011-0009 : VMware hosted product updates, ESX patches and VI Clie...
2	High	VMSA-2011-0012 : VMware ESXi and ESX updates to third party libraries and...
2	High	VMSA-2012-0001 : VMware ESXi and ESX updates to third party library and ...
2	High	VMSA-2012-0009 : VMware Workstation, Player, Fusion, ESXi and ESX patch...
2	High	VMSA-2012-0011 : VMware hosted products and ESXi and ESX patches addr...
1	High	VMSA-2012-0007 : VMware hosted products and ESXi/ESX patches address ...
1	High	VMSA-2011-0004 : VMware ESX/ESXi SLPD denial of service vulnerability an...
1	High	VMSA-2011-0007 : VMware ESXi and ESX Denial of Service and third party u...
1	High	VMSA-2012-0016 : VMware security updates for vSphere API and ESX Servic...
1	High	VMSA-2012-0009 : ESXi and ESX patches address critical security issues (un...

Last Updated: 1 minute ago

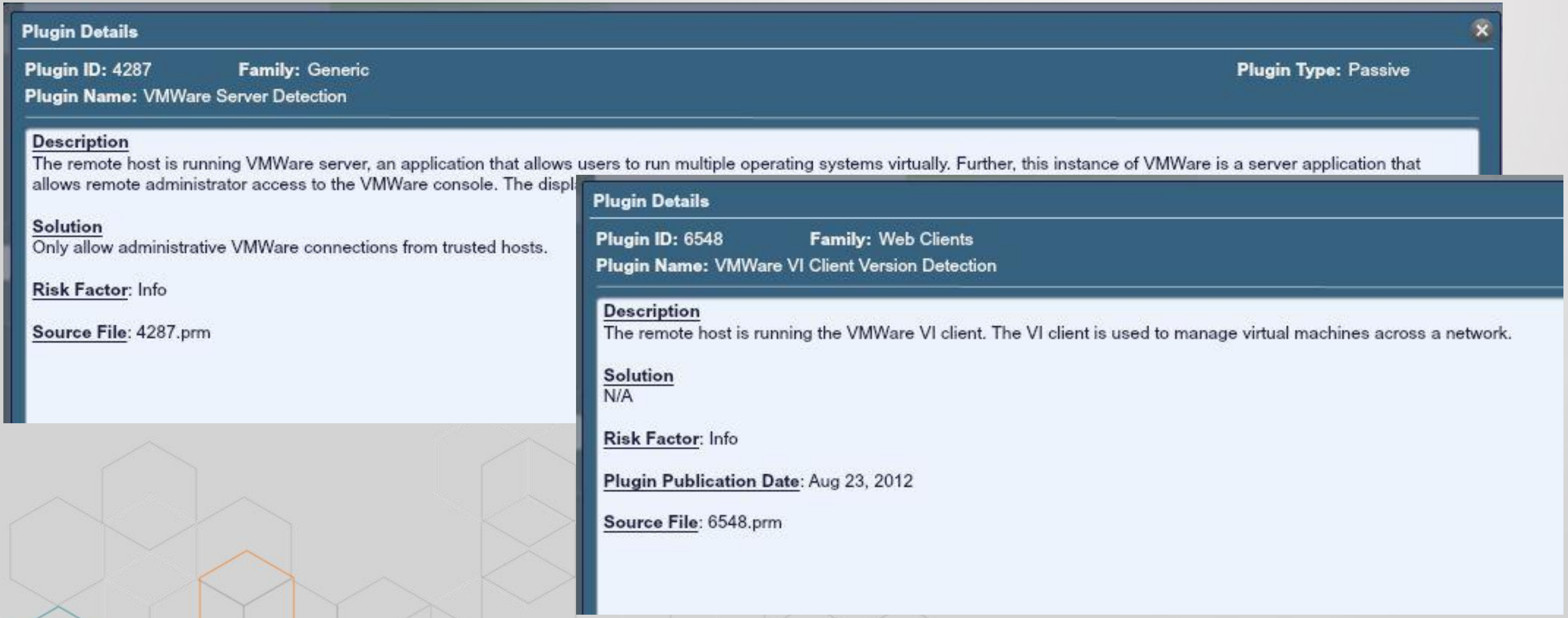
tenable
network security

Solutions: Passive Vulnerability Scanner



Viewing results 1 - 2 out of 2

Plugin ID ▲	Total	Severity	Name	Family
4287	2	Info	VMWare Server Detection	Generic [PVS]
6548	1	Info	VMWare VI Client Version Detection	Web Clients [PVS]



Plugin ID: 4287 **Family:** Generic **Plugin Type:** Passive
Plugin Name: VMWare Server Detection

Description
The remote host is running VMWare server, an application that allows users to run multiple operating systems virtually. Further, this instance of VMWare is a server application that allows remote administrator access to the VMWare console. The displ

Solution
Only allow administrative VMWare connections from trusted hosts.

Risk Factor: Info

Source File: 4287.prm

Plugin ID: 6548 **Family:** Web Clients
Plugin Name: VMWare VI Client Version Detection

Description
The remote host is running the VMWare VI client. The VI client is used to manage virtual machines across a network.

Solution
N/A

Risk Factor: Info

Plugin Publication Date: Aug 23, 2012

Source File: 6548.prm

Tenable Resources

Blog:
http://blog.tenable.com

Podcast:
http://www.tenable.com/podcast

Videos:
http://www.youtube.com/tenablesecurity

Discussion Forum:
https://discussions.nessus.org

Buy Nessus, Perimeter Service, PVS, Training & Bundles:
https://store.tenable.com

Become a Tenable Partner:
http://www.tenable.com/partners

Nessus, PVS, & SecurityCenter Info

For more info on Nessus:

http://www.tenable.com/products/nessus

For more info & to evaluate PVS:

http://www.tenable.com/products/passive-vulnerability-scanner

For more info or to evaluate SecurityCenter Continuous View:

http://www.tenable.com/products/securitycenter-continuous-view

Questions?

????

Thank You!

Contact us:

Paul Asadoorian – paul@nessus.org
Jack Daniel – jdaniel@tenable.com

“Vulnerabilities Exposed” webcast #3:

October 22 at 2 pm EDT

Handling Mobile Threats Before They Cause Loss & Disruption