

Communicating Vulnerabilities to Management: Making the Rubber Meet the Road

"Vulnerabilities Exposed" Webcast Series Part 4

Paul Asadoorian, Jack Daniel, & Renaud Deraison

"Vulnerabilities Exposed" Series

- Final webcast in a 4-part series
 - Part 1: "Reducing Your Patch Cycle to Less Than 5 Days"
 - Part 2: "Addressing the Security Challenges of Virtualization"
 - Part 3: ""BYOD Bring Your Own Devastation Taking On the Mobile Threat"
- Archives & slides:
 www.tenable.com/vulns-exposed

Strategies & solutions for today's common security challenges





Today's Roadmap

- Communicating vulnerability information to management and beyond
- Tips, tricks, and techniques to create interesting reports

Using enterprise tools for complete vulnerability

data management



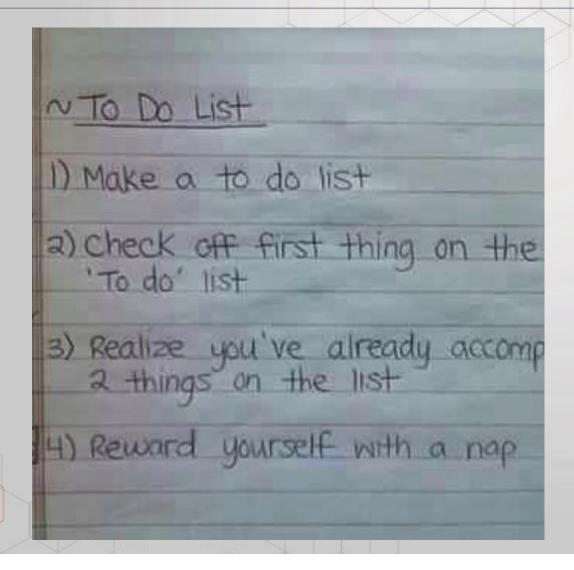


We Are Here to Help





To-Do List





Your (Real) To-Do List

- Create a policy and a process
- Get buy-in from management and all of IT
- Define patch cycles, secure configurations
- Define exceptions to patch cycles
- Who / Where / What / How will you scan?
- Are you patching the right things?



What gaps can I find, and how do I communicate them?



(Anti-Virus, MDM, Patching, Hardening, Penetration Testing, Virtualization, Network Infrastructure)



Policy

We will perform vulnerability scanning on a regular basis. Departments within IT will participate in the process, including groups from Windows, UNIX/Linux, Desktop Management, Virtualization and Networking operations. Management will review the process and results quarterly.





Procedures

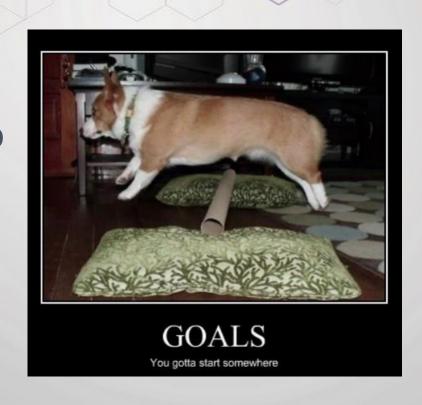
- Each week, all Windows and UNIX/Linux servers will be scanned, administrators will review the results, problems will be remediated, scans will be run again
- Both network and credentialed scans will be run
- Configuration profiles will be defined and checked each week using configuration auditing scans





Goals

- Identify assets
- Discover vulnerabilities
- Report them to people who can fix them
 - Actionable results
- Continuously discover vulnerabilities that remain
- Report progress to management





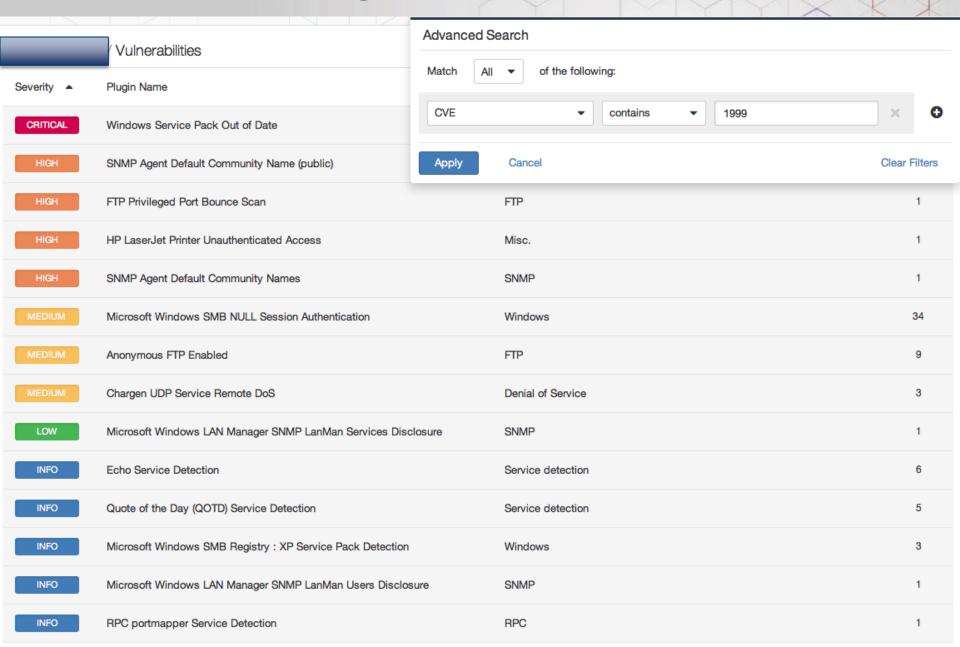
Nessus Can Help

- Result filtering: Carve out the vulnerabilities that matter
- Recast risk: Customize severity for your environment
- Email, filtering, and scheduling: Combine to send actionable results to the right people





Result Filtering: CVE



Result Filtering: Dates

		a / Vulnerabilities	Advanced Search						
	Savority +		Match All ▼ of the following:						
	Severity A	Plugin Name	Patch Publication Date ▼ earlier than ▼ 2013/01/01				×	0	
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)							
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)	Apply	Cancel				Clear Fi	Iters
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (Feb 2012 CPU)		Windows				3	14
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)		Windows				3	34
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)		Windows				3	34
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (Oct 2011 CPU)		Windows				3	34
	CRITICAL	Oracle Java SE Multiple Vulnerabilities (October 2010 CPU)		Windows				3	34
	CRITICAL	Oracle Java JDK / JRE 6 < Update 20 Multiple Vulnerabilities		Windows				3	32
	CRITICAL	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities		Windows				3	32
	CRITICAL	MS12-054: Vulnerabilities in Windows Networking Components 0	Could Allow	Windows : Microso	oft Bulletins			3	31
	CRITICAL	Adobe AIR <= 3.0 Multiple Vulnerabilities (APSB11-28)		Windows				1	0
	CRITICAL	Shockwave Player < 11.5.9.620 (APSB11-01)		Windows					8
	CRITICAL	HP Printer Firmware Signing Disabled		Misc.				:	2
	CRITICAL	HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple	le Vulnerabi	Web Servers				:	2

Patch Matrix

172.26.22.56

Port: 0 / tcp

The following tools were used in this scan.

Nessus

SCCM

WSUS

+Nessus -> SCCM conflicts

```
-ms11-085 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-005 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-058 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-063 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-068 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-069 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-071 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-073 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable -ms12-075 : Nessus reports Vulnerable , SCCM is NOT reporting Vulnerable
```

+Nessus -> WSUS conflicts

```
-ms12-005 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-058 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-068 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-068 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-069 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-071 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-073 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-074 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-075 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable -ms12-075 : Nessus reports Vulnerable , WSUS is NOT reporting Vulnerable
```





Severity Modification

Vulnerabilities / 42263

Low Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in eavesdrop on a Telnet session and obtain credentials or other sensitive information.

Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data stream

Solution

Disable this service and use SSH instead.

Affected Host List

10.0.168.14

Plugin Details

Severity: Low

(Modify)

ID: 42263

Version: \$Revision: 1.6 \$

Type: remote Family: Misc.

Published: 2009/10/27 Modified: 2011/09/15

Risk Information

Risk Factor: Low CVSS Base Score: 2.6

CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N



Severity Modification (2)

a / Vulnerabilities / 42263



Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.

Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Solution

Disable this service and use SSH instead.

Affected Host List

▶ 10.0.168.14	1
▶ 10.0.160.16	1
▶ 10.0.160.1	1
▶ 10.0.152.212	1

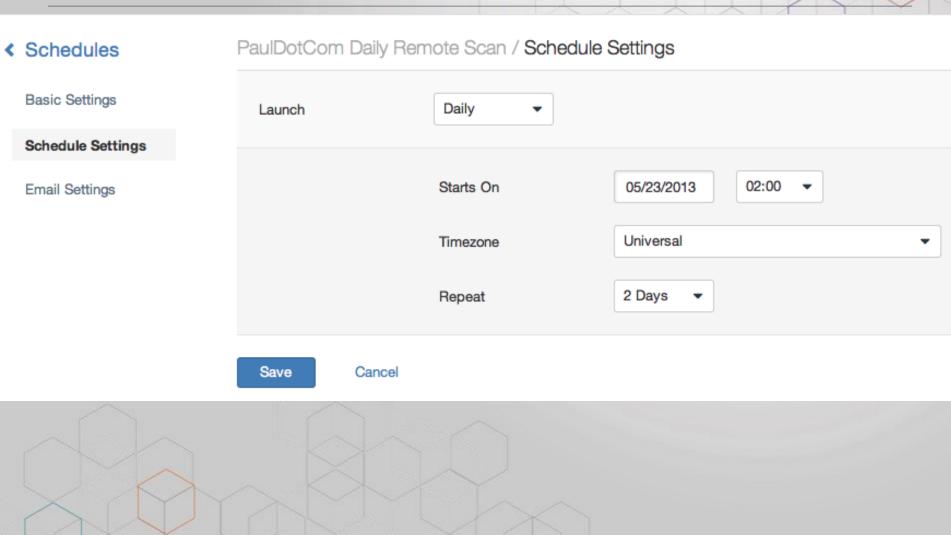


Exploitability

CRITICAL HP Printer Firmware Signing Disabled	Advanced Search	
CRITICAL HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multi	Match Any ▼ of the following:	
CRITICAL HP System Management Homepage < 7.0 Multiple Vulnerabiliti	Exploitability Ease ▼ Is equal to ▼ No exploit is required ▼	× O
CRITICAL Shockwave Player < 11.5.0.602 Multiple Vulnerabilities (APSB0	Exploitability Ease ▼ is equal to ▼ Exploits are available ▼	× O
CRITICAL FreeBSD 'telnetd' Daemon Remote Buffer Overflow	Apply Cancel	Clear Filters
CRITICAL Skype < 6.3.0.105 Multiple Vulnerabilities (credentialed check)		olear Filters
HIGH Flash Player <= 10.3.183.50 / 11.5.502.146 Multiple Vulnerabilit	ties (APSB13 Windows	151
HIGH Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilit	ties (APSB13 Windows	151
Flash Player <= 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilit	ties (APSB12 Windows	149
HIGH Adobe Reader < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities ((APSB13-15) Windows	147
Flash Player <= 11.3.300.270 Code Execution (APSB12-18)	Windows	146
HIGH Adobe Reader < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities ((APSB13-07) Windows	142
MS13-015: Vulnerability in .NET Framework Could Allow Elevation	ion of Privileg Windows : Microsoft Bulletins	115
HIGH Oracle Java JDK / JRE 6 < Update 43 Remote Code Execution	n (Windows) Windows	105

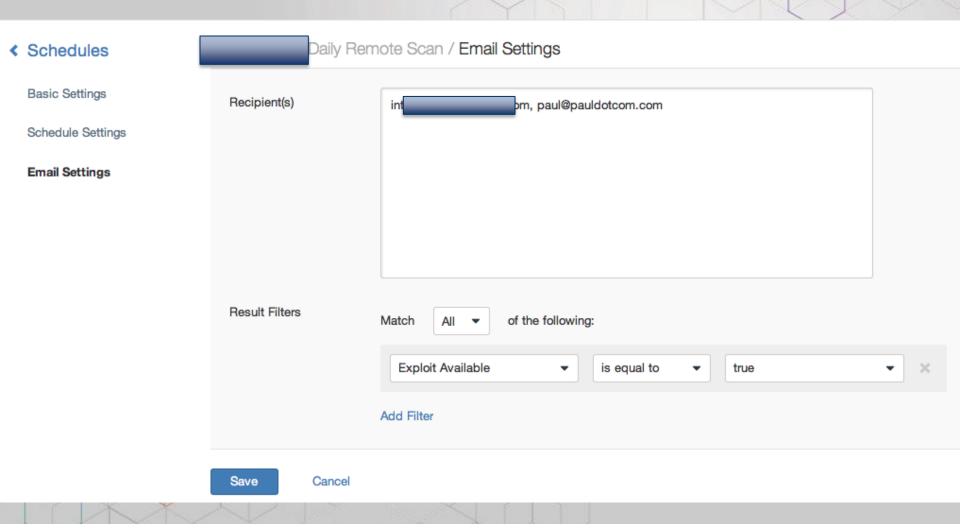


Combine Email, Schedule, & Filtering



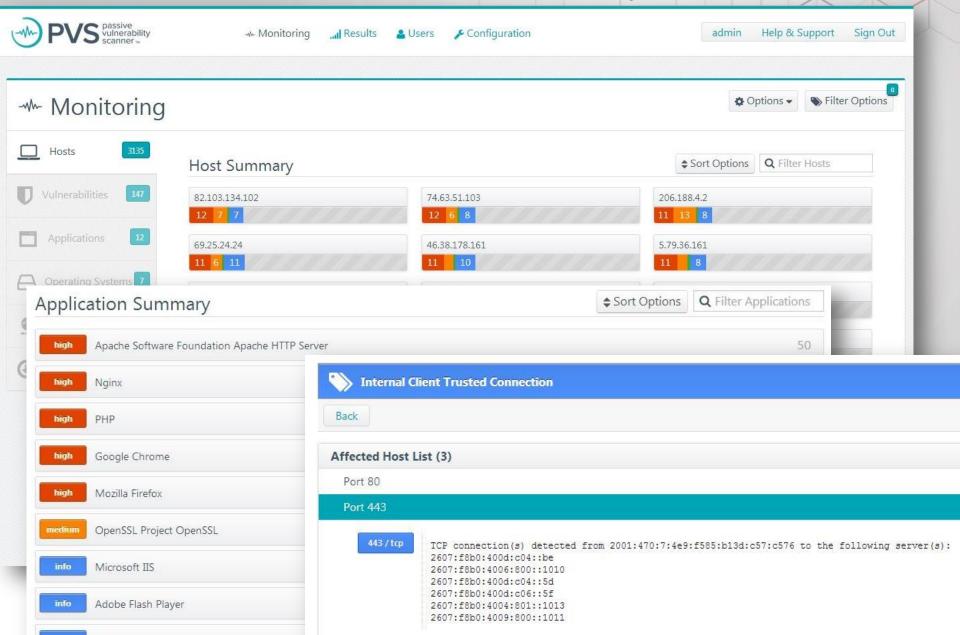


Combine Email, Schedule, & Filtering (2)





Solutions: Passive Vulnerability Scanner



Solutions: SecurityCenter Dashboards

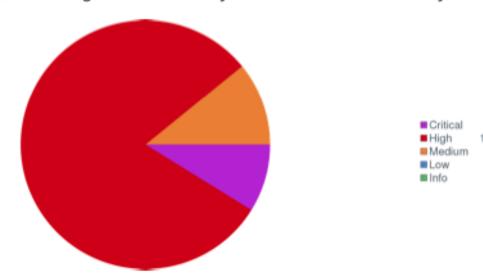
Days Since Mitigation - Vulnerability Count - Patch Date 21 - 60 Days

	Within 30 Days	Within 40 Days	Within 50 Days	Within 60 Days
All Vuins	20	105	4	1
Windows	20	105	4	1
Linux	0	0	0	0
os x	0	0	0	0
CVSS > 5.0	20	104	4	1
Exploitable	7	42	2	0
Web	0	0	0	0

0.00%

0.00%

Days Since Mitigation - Vulnerability Count - Patch Date 21 - 60 Days





Tenable Resources



Blog:

http://blog.tenable.com



Podcast:

http://www.tenable.com/podcast



Videos:

http://www.youtube.com/tenablesecurity



Discussions Forum:

https://discussions.nessus.org



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



Find a Channel Partner:

http://www.tenable.com/partners/find-a-subscription-partner



For More Info or to Evaluate

Nessus:

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

PVS:

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

SecurityCenter Continuous View:

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

Vulnerability Management:

http://static.tenable.com/whitepapers/Vulnerability_Management_Program.pdf



Questions?



Thank You!

Contact us:

Paul Asadoorian – <u>paul@nessus.org</u> Jack Daniel – <u>jdaniel@tenable.com</u>



