Nessus Vulnerability Scanning

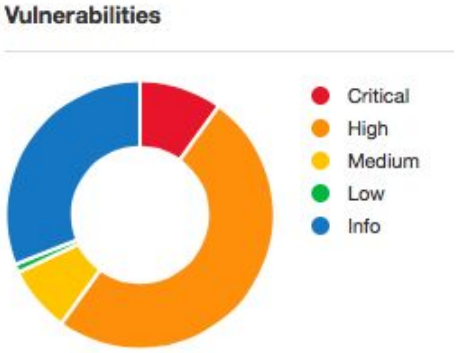
Mengxue Ni, Mengqi He

Introduction

We are using two computers to run the Nessus Scan:

- MacBook Air (OS X 10.9.1)
- HP (Windows 10, Intel Core i7-6500U, 64-bit)

Nessus Result (MacBook Air)



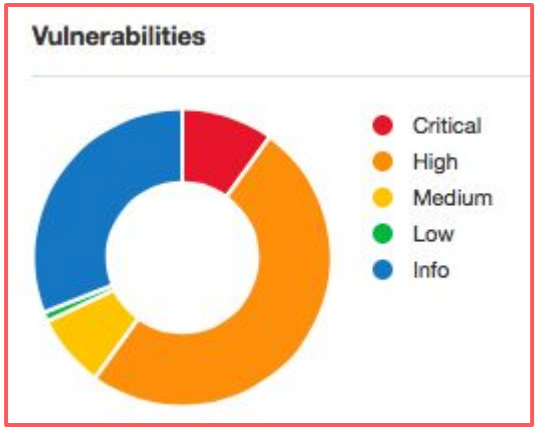
Vulnerabilities	Critical	High	Medium	Low	Total
Vulnerabilities due to low version of OS	9	1			10
Vulnerabilities due to low version of Adobe Photoshop	2				2
Vulnerabilities due to low version of FireFox		26	4		30
Vulnerabilities due to low version of Apple Safari		16	4		20
Vulnerabilities in Microsoft Office allow remote code execution		20			20
Vulnerabilities due to low version of iTunes			1	1	2
Others	2	1	1		4
Total	13	64	10	1	88

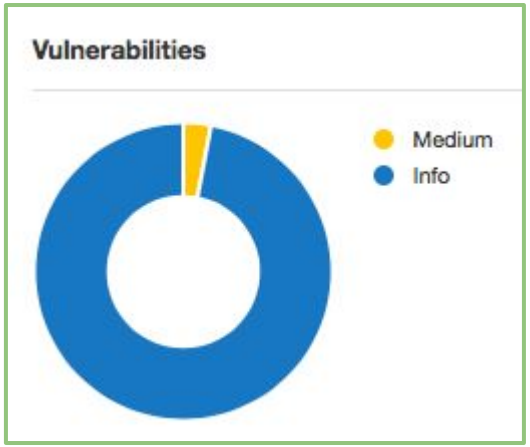
Suggested Solutions (Macbook Air)

- Upgrade OS to Mac OS X 10.11
- Upgrade Firefox to version 44.0.2
- Upgrade Apple Safari to version 7.1.8
- Upgrade Adobe Photoshop to version CC 2015 16.0
- Upgrade iTunes to version 12.5.1
- Update and install patches for Microsoft Office 2011
- Install the vendor-supplied security patch to APPLE-SA-2014-12-22-1
- Purchase or generate a proper certificate for the service

Re-Scan Result

- **Pre-update: 88**
- **Pro-update: 1**





Nessus Result (HP)

Severity	Plugin Name
MEDIUM	SMB Signing Disabled
MEDIUM	SSL Certificate Cannot Be Trusted

SMB Signing Disabled :
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

SSL Certificate Cannot Be Trusted :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

Suggested Solutions (HP)

Solution for SMB Signing Disabled

- Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.

Solution for SSL Certificate Cannot Be Trusted

- Purchase or generate a proper certificate for this service.

Conclusion

- MacBook Air was bought in 2012 and was not used frequently. It contains 13 critical, 64 high, 10 medium and 1 low vulnerabilities.

- HP Windows 10 was bought only half year and used daily. It only contains 2 median vulnerabilities.