JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Server and Host Vulnerabilities

VULNERABILITY MANAGEMENT

Server and Host

- Missing Patches
- Unsupported Software (OS/Apps)
- Buffer Overflows
- Privilege Escalation
- Arbitrary Code Execution
- Insecure Protocol Use
- Debugging Modes

Missing Patches

- One of the most common issues found
- Comes from improper patch management

Plugin ID: 40563 **Port / Service:** general/tcp **Severity:** High

Plugin Name: MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (Mac OS X)

Synopsis

Arbitrary code can be executed on the remote host through Microsoft Remote Desktop Connection.

Description

The remote host contains a version of the Remote Desktop client that contains several vulnerabilities that may allow an attacker to execute arbirtary code on the remote host.

To exploit these vulnerabilities, an attacker would need to trick a user of the remote host into connecting to a rogue RDP server.

Solution

Microsoft has released a patch for Remote Desktop Client for Mac OS X :

http://www.microsoft.com/technet/security/Bulletin/MS09-044.mspx

Unsupported Software

- Software vendors don't support software forever, they have an "end of life" date

- After this date, no more patches are released for the software

Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows Vista	Service Pack 2	April 10, 2012	April 11, 2017
Windows 7 *	Service Pack 1	January 13, 2015	January 14, 2020
Windows 8	Windows 8.1	January 9, 2018	January 10, 2023
Windows 10 **	See Available Updates	October 13, 2020	October 14, 2025

Buffer Overflows

- Occurs when the attacker manipulates a program to place more data into memory than it is allocated for causing overflow
- Another specific type is integer overflow
- These vulnerabilities tend to exist for a long time, but are corrected by a patch
- In 2015, over 85% of the data breaches were cause by buffer overflows

Privilege Escalation

- Occurs when an attacker upgrades their level of access to an admin or root user
- For example, CVE-2016-7255 is an example in Windows Vista, 2008, 7, 8.1, 10, and 2016 machines
- Kernel-mode drivers are exploited to allow local users to become an admin

Arbitrary Code Execution

- Allows attacker to run software on a targeted victim machine

- Remote code execution is worse, because it allows it to occur over network

48762 - MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution [-/+]

Synopsis

The remote Windows host may be vulnerable to code execution attacks.

Description

The remote host is missing Microsoft KB2264107 or an associated registry change, which provides a mechanism for mitigating binary planting or DLL preloading attacks.

Insecurely implemented applications look in their current working directory when resolving DLL dependencies. If a malicious DLL with the same name as a required DLL is located in the application's current working directory, the malicious DLL will be loaded.

A remote attacker could exploit this issue by tricking a user into accessing a vulnerable application via a network share or WebDAV folder where a malicious DLL resides, resulting in arbitrary code execution.

See Also

http://technet.microsoft.com/en-us/security/advisory/2269637

http://www.nessus.org/u?960d4ef0

Insecure Protocol Use

- Older protocols not design for security

- FTP, Telnet, SMBv1, …

97086 - Server Message Block (SMB) Protocol Version 1 Enabled [-/+]

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

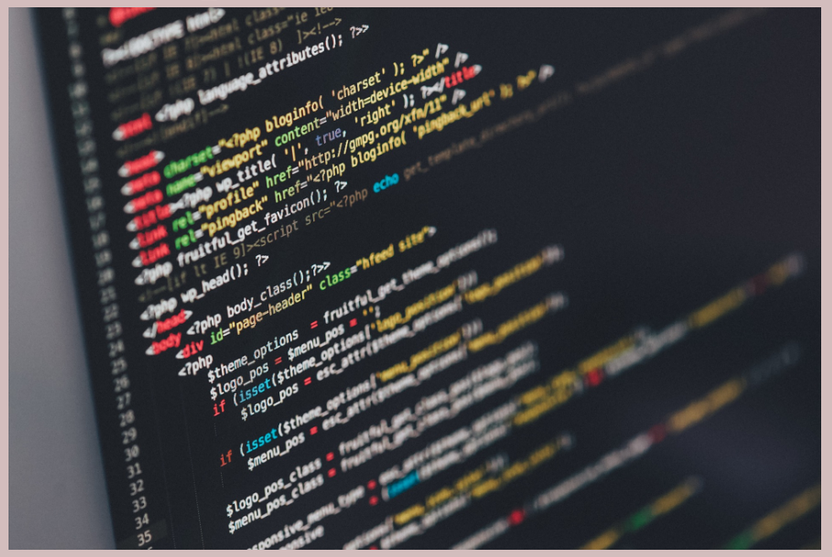
Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Debugging Modes

- Debugging modes give lots of information to developers, but should be disabled prior to server and code deployment

- Debugging information could give attackers a lot of information during a reconnaissance



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE