JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Interpreting Scan Results

VULNERABILITY MANAGEMENT

Importance of Scan Results

- Scanners do a great job of automating the identification of vulnerabilities

- …but, a trained analyst is required to understand the implications of those vulnerabilities
  - Eliminating false positives
  - Finding root causes
  - Prioritizing remediation actions

Scan Results

Nessus™

Nessus Scan Report

Fri, 14 Jul 2017 14:45:49 Eastern Standard Time

Table Of Contents

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Detailed Scan Results

97833 (2) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

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

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users 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.

Risk Factor

Critical

Synopsis and Description

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

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

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Solution

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users 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.

Risk Factor and CVSS Score

Risk Factor
Critical
CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v3.0 Temporal Score
8.8 (CVSS:3.0/E:P/RL:O/RC:C)
CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS Temporal Score
7.8 (CVSS2#E:POC/RL:OF/RC:C)
STIG Severity
I

References

References			
BID	96709	XREF	IAVA:2017-A-0065
BID	96707	XREF	MSFT:MS17-010
BID	96706	XREF	EDB-ID:41987
BID	96705	XREF	EDB-ID:41891
BID	96704	XREF	OSVDB:155635
BID	96703	XREF	OSVDB:155634
CVE	CVE-2017-0148	XREF	OSVDB:155620
CVE	CVE-2017-0147	XREF	OSVDB:153678
CVE	CVE-2017-0146	XREF	OSVDB:153677
CVE	CVE-2017-0145	XREF	OSVDB:153676
CVE	CVE-2017-0144	XREF	OSVDB:153675
CVE	CVE-2017-0143	XREF	OSVDB:153674
		XREF	OSVDB:153673

Exploitable, Plugin, and Hosts

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2017/03/20, Modification date: 2017/06/28

Hosts

192.168.15.112 (tcp/445)

192.168.15.113 (tcp/445)