Windows 7 After Installs

Vulnerabilities & Remedations

Report generated by Nessus™ Wed, 10 Jan 2018 22:31:35 EST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

53514 (1) - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-030

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

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

BID	47242
CVE	CVE-2011-0657
MSKB	2509553
XREF	OSVDB:71780
XREF	IAVA:2011-A-0039
XREF	MSFT:MS11-030

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2011/04/21, Modified: 2017/08/30

Plugin Output

192.168.1.70 (udp/5355)

97833 (1) - 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

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

9.5 (CVSS:3.0/E:F/RL:U/RC:X)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

9.5 (CVSS2#E:F/RL:U/RC:ND)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215

MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	OSVDB:153673
XREF	OSVDB:153674
XREF	OSVDB:153675
XREF	OSVDB:153676
XREF	OSVDB:153677
XREF	OSVDB:153678
XREF	OSVDB:155620
XREF	OSVDB:155634
XREF	OSVDB:155635
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2017/03/20, Modified: 2017/09/07

Plugin Output

192.168.1.70 (tcp/445)

57608 (1) - SMB Signing Disabled

Synopsis

Signing is not required on the remote SMB server.

Description

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.

See Also

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

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'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Published: 2012/01/19, Modified: 2016/12/09

Plugin Output

192.168.1.70 (tcp/445)

10335 (7) - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/10/24

Plugin Output

192.168.1.70 (tcp/135)

```
Port 135/tcp was found to be open
```

192.168.1.70 (tcp/139)

```
Port 139/tcp was found to be open
```

192.168.1.70 (tcp/445)

```
Port 445/tcp was found to be open
```

192.168.1.70 (tcp/554)

```
Port 554/tcp was found to be open
```

192.168.1.70 (tcp/2869)

```
Port 2869/tcp was found to be open
```

192.168.1.70 (tcp/8008)

```
Port 8008/tcp was found to be open
```

192.168.1.70 (tcp/8080)

```
Port 8080/tcp was found to be open
```

10736 (7) - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

192.168.1.70 (tcp/135)

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc044140

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc044140

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-026fe47f50c8c0afcb

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc046541

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc046541

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-a42d84184fae736db5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8174bb16-571b-4c38-8386-1102b449044a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9bf48bc78e355945d5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a2d47257-12f7-4beb-8981-0ebfa935c407, version 1.0 [...]
```

192.168.1.70 (tcp/445)

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\EXPLOITME

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\EXPLOITME
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\EXPLOITME

Object UUID : 00000000-0000-0000-0000-000000000000
 [...]
```

192.168.1.70 (tcp/49152)

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.1.70
```

192.168.1.70 (tcp/49153)

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
```

```
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.70
```

192.168.1.70 (tcp/49154)

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
```

```
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.70
```

192.168.1.70 (tcp/49155)

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.70

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.70
```

192.168.1.70 (tcp/49156)

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.70
```

11011 (2) - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

192.168.1.70 (tcp/139)

```
An SMB server is running on this port.
```

192.168.1.70 (tcp/445)

```
A CIFS server is running on this port.
```

10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/09/27

Plugin Output

192.168.1.70 (udp/137)

```
The following 4 NetBIOS names have been gathered :

 EXPLOITME        = Computer name
 WORKGROUP        = Workgroup / Domain name
 EXPLOITME        = File Server Service
 WORKGROUP        = Browser Service Elections

The remote host has the following MAC address on its adapter :

   08:00:27:45:e7:18
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

192.168.1.70 (udp/0)

```
For your information, here is the traceroute from 192.168.1.65 to 192.168.1.70 :
192.168.1.65
192.168.1.70

Hop Count: 1
```

10394 (1) - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

https://support.microsoft.com/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2017/11/06

Plugin Output

192.168.1.70 (tcp/445)

```
- NULL sessions are enabled on the remote host.
```

10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

192.168.1.70 (tcp/445)

```
The remote Operating System is : Windows 7 Ultimate 7601 Service Pack 1
The remote native LAN manager is : Windows 7 Ultimate 6.1
The remote SMB Domain Name is : EXPLOITME
```

10919 (1) - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Published: 2002/03/19, Modified: 2014/06/04

Plugin Output

192.168.1.70 (tcp/0)

```
Port 8008 was detected as being open initialy but was found unresponsive later.
 It is now unresponsive
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/18, Modified: 2017/06/08

Plugin Output

192.168.1.70 (tcp/2869)

```
A web server seems to be running on this port.
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2003/12/09, Modified: 2017/08/29

Plugin Output

192.168.1.70 (tcp/0)

```
Remote operating system : Microsoft Windows 7 Ultimate
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows 7 Ultimate
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

192.168.1.70 (tcp/0)

```
192.168.1.70 resolves as ExploitMe.lan.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

192.168.1.70 (tcp/0)

```
Information about this scan :

Nessus version : 7.0.0
Plugin feed version : 201801091615
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Copy of Advanced Scan
Scanner IP : 192.168.1.65
Port scanner(s) : nessus_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/1/10 22:21 EST
Scan duration : 584 sec
```

22964 (1) - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2017/07/07

Plugin Output

192.168.1.70 (tcp/8008)

```
A web server is running on this port.
```

24786 (1) - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Published: 2007/03/12, Modified: 2013/01/07

Plugin Output

192.168.1.70 (tcp/0)

```
It was not possible to connect to '\\EXPLOITME\ADMIN$' with the supplied credentials.
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

192.168.1.70 (tcp/0)

26917 (1) - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/10/04, Modified: 2011/03/27

Plugin Output

192.168.1.70 (tcp/445)

```
Could not connect to the registry because:
Could not connect to \winreg
```

35711 (1) - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2009/02/19, Modified: 2017/06/12

Plugin Output

192.168.1.70 (udp/1900)

```
The device responded to an SSDP M-SEARCH request with the following locations :

    http://192.168.1.70:2869/upnphost/udhisapi.dll?content=uuid:46b03eea-d84c-4ebf-abca-020b5493b184

And advertises these unique service names :

    uuid:46b03eea-d84c-4ebf-abca-020b5493b184::upnp:rootdevice
    uuid:46b03eea-d84c-4ebf-abca-020b5493b184::urn:schemas-upnp-org:device:MediaServer:1
    uuid:46b03eea-d84c-4ebf-abca-020b5493b184::urn:schemas-upnp-org:service:ContentDirectory:1
    uuid:46b03eea-d84c-4ebf-
abca-020b5493b184::urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
```

35712 (1) - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2009/02/19, Modified: 2017/06/12

Plugin Output

192.168.1.70 (tcp/2869)

```
Here is a summary of http://192.168.1.70:2869/upnphost/udhisapi.dll?content=uuid:46b03eea-d84c-4ebf-
abca-020b5493b184 :

deviceType: urn:schemas-upnp-org:device:MediaServer:1
friendlyName: EXPLOITME: msfadmin:
manufacturer: Microsoft Corporation
manufacturerURL: http://www.microsoft.com
modelName: Windows Media Player Sharing
modelName: Windows Media Player Sharing
modelNumber: 12.0
modelURL: http://go.microsoft.com/fwlink/?LinkId=105926
serialNumber: {BB07903D-7E3D-4E8E-B846-F1BEDCBE8FC6}
ServiceID: urn:upnp-org:serviceId:ConnectionManager
 serviceType: urn:schemas-upnp-org:service:ConnectionManager:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:46b03eea-d84c-4ebf-abca-020b5493b184+urn:upnp-
org:serviceId:ConnectionManager
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:46b03eea-d84c-4ebf-abca-020b5493b184+urn:upnp-
org:serviceId:ConnectionManager
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:ef5b3ee8-30f9-451d-a866-6a1ed55f284d
ServiceID: urn:upnp-org:serviceId:ContentDirectory
 serviceType: urn:schemas-upnp-org:service:ContentDirectory:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:46b03eea-d84c-4ebf-abca-020b5493b184+urn:upnp-
org:serviceId:ContentDirectory
```

```
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:46b03eea-d84c-4ebf-abca-020b5493b184+urn:upnp-
org:serviceId:ContentDirectory
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:8ea7b36c-f9bc-4ebe-ab60-0e4c4be27e90
ServiceID: urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 serviceType: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:46b03eea-d84c-4ebf-
abca-020b5493b184+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:46b03eea-d84c-4ebf-
abca-020b5493b184+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:da188c20-159e-4c31-93be-b6e1aa083e64
```

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

http://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/02/19, Modified: 2017/11/17

Plugin Output

192.168.1.70 (tcp/0)

```
The following card manufacturers were identified :

08:00:27:45:e7:18 : PCS Systemtechnik GmbH
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

192.168.1.70 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::ultimate
```

46180 (1) - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Published: 2010/04/29, Modified: 2017/04/27

Plugin Output

192.168.1.70 (tcp/0)

```
The following hostnames point to the remote host :
  - exploitme
```

53513 (1) - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2011/04/21, Modified: 2012/03/05

Plugin Output

192.168.1.70 (udp/5355)

```
According to LLMNR, the name of the remote host is 'ExploitMe'.
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

192.168.1.70 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 99
```

96982 (1) - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

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.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

192.168.1.70 (tcp/445)

```
The remote host supports SMBv1.
```

100871 (1) - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

192.168.1.70 (tcp/445)

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```