Nessus Report

Nessus Scan Report

Sat, 29 Oct 2016 05:40:30 CLST

Table Of Contents

Vulnerabilities By Host

192.168.87.129

Scan Information

Start time:	Sat Oct 29 05:37:25 2016
End time:	Sat Oct 29 05:40:30 2016

Host Information

Netbios Name:	VUL1-XP
IP:	192.168.87.129
MAC Address:	00:0c:29:79:54:34
OS:	Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

Results Summary

Critical	High	Medium	Low	Info	Total
2	4	6	2	36	50

Results Details

0/icmp

11197 - Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Synopsis

The remote host appears to leak memory in network packets.

Description

The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.
Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

See Also

http://www.nessus.org/u?719c90b4

Solution

Contact the network device driver's vendor for a fix.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	6535
CVE	CVE-2003-0001
XREF	OSVDB:3873

Plugin Information:

Publication date: 2003/01/14, Modification date: 2015/01/21

Ports

icmp/0

```
Padding observed in one frame :

  0x00:  18 48 CC 80 18 44 1E 69 6F 00 00 01 01 08 0A 00    .H...D.io.......
  0x10:  00                                                 .

Padding observed in another frame :

  0x00:  61 A6 A2 80 10 44 6E 72 BA 00 00 01 01 08 0A 00    a....Dnr........
  0x10:  00                                                 .
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is 2 seconds.
```

0/tcp

24786 - 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:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

```
It was not possible to connect to '\\VUL1-XP\ADMIN$' with the supplied credentials.
```

25220 - 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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - 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:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

```
The following card manufacturers were identified :

00:0c:29:79:54:34 : VMware, Inc.
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```
The remote host is a VMware virtual machine.
```

11936 - 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:

Publication date: 2003/12/09, Modification date: 2016/02/24

Ports

tcp/0

```
Remote operating system : Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-IIS/5.1
NTP:!:unknown
SinFP:
   P1:B11113:F0x12:W16616:O0204ffff:M1460:
   P2:B11113:F0x12:W17520:O0204ffff010303000101080a0000000000000000001010402:M1460:
   P3:B11021:F0x04:W0:O0:M0
   P4:6900_7_p=443
SMTP:220 VUL1-XP Microsoft ESMTP MAIL Service, Version: 6.0.2600.2180 ready at  Sat, 29 Oct 2016
 11:37:48 +0200
RDP:000000000f0000001000010008000100090000000100100010 0010


The remote host is running one of these operating systems :
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is 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/cpe.cfm

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Ports

tcp/0

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

  cpe:/o:microsoft:windows_xp::sp2 -> Microsoft Windows XP Service Pack 2
  cpe:/o:microsoft:windows_xp::sp3 -> Microsoft Windows XP Service Pack 3
  cpe:/o:microsoft:windows

Following application CPE matched on the remote system :

  cpe:/a:microsoft:iis:5.1 -> Microsoft IIS 5.1
```

54615 - 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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

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

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Publication date: 2013/07/08, Modification date: 2016/10/26

Ports

tcp/0

```
. You need to take the following 3 actions :

[ MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
 (18502) ]

+ Action to take : Microsoft has released a set of patches for Windows 2000, XP and 2003.


[ MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of
 Service (981832) (uncredentialed check) (45517) ]

+ Action to take : Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as
 well as Exchange Server 2000, 2003, 2007, and 2010 :

http://technet.microsoft.com/en-us/security/bulletin/MS10-024

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).



[ MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
 (uncredentialed check) (58435) ]

+ Action to take : Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7,
 and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this
 vulnerability for Windows 2000.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

19506 - 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:

Publication date: 2005/08/26, Modification date: 2016/04/08

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.9.0
Plugin feed version : 201610272215
Scanner edition used : Nessus
```

```
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.87.128
Port scanner(s) : nessus_syn_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 : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/10/29 5:37 CLST
Scan duration : 185 sec
```

0/udp

10287 - 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:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.87.128 to 192.168.87.129 :
192.168.87.128
192.168.87.129
```

25/tcp

45517 - MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)

Synopsis

The remote mail server may be affected by multiple vulnerabilities.

Description

The installed version of Microsoft Exchange / Windows SMTP Service is affected by at least one vulnerability :
- Incorrect parsing of DNS Mail Exchanger (MX) resource records could cause the Windows Simple Mail Transfer Protocol (SMTP) component to stop responding until the service is restarted. (CVE-2010-0024)
- Improper allocation of memory for interpreting SMTP command responses may allow an attacker to read random email message fragments stored on the affected server.
(CVE-2010-0025)

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as well as Exchange Server 2000, 2003, 2007, and 2010 :
http://technet.microsoft.com/en-us/security/bulletin/MS10-024

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

II

References

BID	39381
CVE	CVE-2010-0024
CVE	CVE-2010-0025
XREF	OSVDB:63738
XREF	OSVDB:63739
XREF	MSFT:MS10-024
XREF	IAVB:2010-B-0029

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2010/04/13, Modification date: 2014/07/11

Ports

tcp/25

```
The remote version of the smtpsvc.dll is 6.0.2600.2180 versus 6.0.2600.3680.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/25

```
Port 25/tcp was found to be open
```

22964 - 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:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/25

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

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/25

```
Remote SMTP server banner :

220 VUL1-XP Microsoft ESMTP MAIL Service, Version: 6.0.2600.2180 ready at  Sat, 29 Oct 2016
 11:37:48 +0200
```

80/tcp

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Risk Factor

High

CVSS Base Score

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

Plugin Information:

Publication date: 2008/10/21, Modification date: 2015/09/24

Ports

tcp/80

```
Product                : Microsoft IIS 5.1
Server response header : Microsoft-IIS/5.1
Support ended          : 2014-04-08
```

```
Supported versions     : Microsoft IIS 8.5 / 8.0 / 7.5 / 7.0 / 6.0
Additional information : http://support.microsoft.com/lifecycle/?p1=2096
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/05/04

Ports

tcp/80

```
Use the URLScan tool to deny HTTP TRACE requests or to permit only the
methods needed to meet site requirements and policy.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1600231059.html HTTP/1.1
Connection: Close
Host: 192.168.87.129
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sat, 29 Oct 2016 09:38:44 GMT
Content-Type: message/http
Content-Length: 316


TRACE /Nessus1600231059.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.87.129
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - 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:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/80

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods  COPY  GET  HEAD  LOCK  PROPFIND  SEARCH  TRACE
    UNLOCK OPTIONS are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Microsoft-IIS/5.1
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.
If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information:

Publication date: 2003/03/20, Modification date: 2011/03/14

Ports

tcp/80

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
 PROPPATCH, LOCK, UNLOCK, SEARCH
Headers :

  Server: Microsoft-IIS/5.1
  Content-Location: http://192.168.87.129/index.html
  Date: Sat, 29 Oct 2016 09:38:54 GMT
  Content-Type: text/html
  Accept-Ranges: bytes
  Last-Modified: Thu, 25 Jun 2015 11:46:48 GMT
  ETag: "04279e3cafd01:9bd"
  Content-Length: 134
```

123/udp

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server with an insecure configuration is listening on the remote host.

Description

An NTP server with an insecure configuration is listening on port 123.
It provides information about its version, current date, current time, and it may also provide system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2015/06/12

Ports

udp/123

```
Version : unknown
```

135/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/135

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

443/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/443

```
Port 443/tcp was found to be open
```

445/tcp

35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Synopsis

It is possible to crash the remote host due to a flaw in SMB.

Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

See Also

http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

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)

References

BID	31179
BID	33121
BID	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
XREF	OSVDB:48153
XREF	OSVDB:52691
XREF	OSVDB:52692
XREF	MSFT:MS09-001
XREF	CWE:399

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2009/01/13, Modification date: 2016/10/18

Ports

tcp/445

18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host.

An attacker does not need to be authenticated to exploit this flaw.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms05-027

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

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)

References

BID	13942
CVE	CVE-2005-1206
XREF	OSVDB:17308
XREF	MSFT:MS05-027

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2005/06/16, Modification date: 2013/11/04

Ports

tcp/445

22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.
In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms06-035

https://www.tenable.com/security/research/tra-2006-01

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	18863

BID	18891
CVE	CVE-2006-1314
CVE	CVE-2006-1315
XREF	OSVDB:27154
XREF	OSVDB:27155
XREF	TRA:TRA-2006-01
XREF	MSFT:MS06-035

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2006/07/12, Modification date: 2015/10/07

Ports

tcp/445

26920 - Microsoft Windows SMB NULL Session Authentication

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).
Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

http://support.microsoft.com/kb/q143474/

http://support.microsoft.com/kb/q246261/

http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Solution

Apply the following registry changes per the referenced Technet advisories :
Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1
Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes
Reboot once the registry changes are complete.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.2 (CVSS2#E:U/RL:U/RC:ND)

References

BID	494
CVE	CVE-1999-0519
CVE	CVE-1999-0520

CVE	CVE-2002-1117
XREF	OSVDB:299
XREF	OSVDB:8230

Plugin Information:

Publication date: 2007/10/04, Modification date: 2012/02/29

Ports

tcp/445

```
It was possible to bind to the \browser pipe
```

57608 - 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:

Publication date: 2012/01/19, Modification date: 2016/06/29

Ports

tcp/445

11011 - 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:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

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

10150 - 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:

Publication date: 1999/10/12, Modification date: 2016/02/26

Ports

tcp/445

```
The following 2 NetBIOS names have been gathered :

 VUL1-XP          = Computer name
 VUL1-XP          = Workgroup / Domain name
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

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

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2016/01/13

Ports

tcp/445

```
The remote Operating System is : Windows 5.1
The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : VUL1-XP
```

10394 - 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

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2016/03/11

Ports

tcp/445

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/445

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

26917 - 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:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

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

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.
By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/11/06, Modification date: 2011/03/27

Ports

tcp/445

```
The following 2 NetBIOS names have been gathered :

 VUL1-XP          = Computer name
 VUL1-XP          = Workgroup / Domain name
```

3306/tcp

10481 - MySQL Unpassworded Account Check

Synopsis

The remote database server can be accessed without a password.

Description

It is possible to connect to the remote MySQL database server using an unpassworded account. This may allow an attacker to launch further attacks against the database.

See Also

http://dev.mysql.com/doc/refman/5.0/en/default-privileges.html

Solution

Disable or set a password for the affected account.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

7.5 (CVSS2#E:H/RL:U/RC:ND)

References

BID	11704
CVE	CVE-2002-1809
CVE	CVE-2004-1532
XREF	OSVDB:380
XREF	OSVDB:16026
XREF	OSVDB:101006

Plugin Information:

Publication date: 2000/07/27, Modification date: 2015/09/24

Ports

tcp/3306

```
The anonymous account does not have a password.

Here is the list of databases on the remote server :

  - information_schema
  - test
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/3306

```
Port 3306/tcp was found to be open
```

11153 - 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:

Publication date: 2002/11/18, Modification date: 2016/05/26

Ports

tcp/3306

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

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/13, Modification date: 2013/01/07

Ports

tcp/3306

```
Version  : 5.0.15-nt
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

3389/tcp

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.
If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.
This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.
Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.
Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
XREF	OSVDB:80000
XREF	OSVDB:80004

XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2012/03/22, Modification date: 2016/10/20

Ports

tcp/3389

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.
Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :
3. High
4. FIPS Compliant

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2012/01/25, Modification date: 2016/10/20

Ports

tcp/3389

```
The terminal services encryption level is set to :

2. Medium
```

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.
This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

http://www.oxid.it/downloads/rdp-gbu.pdf

http://www.nessus.org/u?e2628096

http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.6 (CVSS2#E:F/RL:W/RC:ND)

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Plugin Information:

Publication date: 2005/06/01, Modification date: 2014/03/04

Ports

tcp/3389

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :
4. FIPS Compliant

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2008/02/11, Modification date: 2016/10/20

Ports

tcp/3389

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/3389

```
Port 3389/tcp was found to be open
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).
If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.
Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information:

Publication date: 2002/04/20, Modification date: 2014/06/06

Ports

tcp/3389

66173 - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.
While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/04/22, Modification date: 2016/10/20

Ports

tcp/3389

```
It was possible to gather the following screenshot of the remote login screen.
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 19% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check): Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as well as Exchange Server 2000, 2003, 2007, and 2010 : http://technet.microsoft.com/en-us/security/bulletin/MS10-024	2	1
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check): Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.	2	1