



## scan4

---

Report generated by Nessus<sup>TM</sup>

Wed, 10 Jul 2019 08:47:39 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 10.0.0.131.....4

### Remediations

- Suggested Remediations..... 64

---

## **Vulnerabilities by Host**

---

10.0.0.131

2

CRITICAL

2

HIGH

4

MEDIUM

1

LOW

38

INFO

## Scan Information

Start time: Wed Jul 10 08:43:40 2019

End time: Wed Jul 10 08:47:39 2019

## Host Information

Netbios Name: IEWIN7

IP: 10.0.0.131

MAC Address: 00:0C:29:43:01:3E

OS: Microsoft Windows 7 Enterprise

## Vulnerabilities

**51956 - MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (unauthenticated check)**

## Synopsis

The FTP service running on the remote host has a memory corruption vulnerability.

## Description

The IIS FTP service running on the remote host has a heap-based buffer overflow vulnerability. The 'TELNET\_STREAM\_CONTEXT::OnSendData'

function fails to properly sanitize user input, resulting in a buffer overflow.

An unauthenticated, remote attacker can exploit this to execute arbitrary code.

## See Also

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-004>

## Solution

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

## 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

---

9.0 (CVSS:3.0/E:F/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

---

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

### References

---

BID	45542
CVE	CVE-2010-3972
MSKB	2489256
XREF	EDB-ID:15803
XREF	MSFT:MS11-004

### Exploitable With

---

Core Impact (true)

### Plugin Information

---

Published: 2011/02/11, Modified: 2018/11/15

### Plugin Output

---

tcp/21

## 97833 - 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

---

<http://www.nessus.org/u?68fc8eff>

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

<http://www.nessus.org/u?065561d0>

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

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

<http://www.nessus.org/u?b9d9ebf9>

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

<http://www.nessus.org/u?234f8ef8>

<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**

---

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

**CVSS v3.0 Temporal Score**

---

7.7 (CVSS:3.0/E:H/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**

---

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

**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	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

### Exploitable With

---

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

### Plugin Information

---

Published: 2017/03/20, Modified: 2019/02/26

### Plugin Output

---

tcp/445



### Synopsis

It is possible to log into the remote host.

### Description

The remote host is running one of the Microsoft Windows operating systems or the SAMBA daemon. It was possible to log into it as a guest user using a random account.

### Solution

In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'. Disable the Guest account if applicable.

If the SAMBA daemon is running, double-check the SAMBA configuration around guest user access and disable guest access if appropriate

### Risk Factor

High

### CVSS Base Score

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

### References

CVE CVE-1999-0505

### Exploitable With

Metasploit (true)

### Plugin Information

Published: 2007/10/04, Modified: 2018/09/17

### Plugin Output

tcp/445

## 10166 - Windows NT FTP 'guest' Account Present

### Synopsis

There is a 'guest' account on the remote FTP server.

### Description

The remote Windows host has a 'guest' FTP account enabled. This could allow a remote attacker to upload or download arbitrary files on the remote host.

Note that this plugin only tests for guest accounts over FTP.

### Solution

Disable this FTP account.

### Risk Factor

High

### 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 Base Score

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

### References

BID	87877
CVE	CVE-1999-0546

### Plugin Information

Published: 1999/06/22, Modified: 2018/08/13

### Plugin Output

tcp/21

```
Nessus was able to gain access using the following set of credentials :
```

```
Username : guest
Password : The guest account has no password
```

## 10079 - Anonymous FTP Enabled

### Synopsis

Anonymous logins are allowed on the remote FTP server.

### Description

Nessus has detected that the FTP server running on the remote host allows anonymous logins. Therefore, any remote user may connect and authenticate to the server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.

### Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS Base Score

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

### References

BID	83206
CVE	CVE-1999-0497

### Plugin Information

Published: 1999/06/22, Modified: 2018/10/10

### Plugin Output

tcp/21

```
The contents of the remote FTP root are :
07-10-19 02:15AM                282 desktop.ini
```

## 62940 - MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)

### Synopsis

The Microsoft IIS service running on the remote system contains flaws that could lead to an unauthorized information disclosure.

### Description

The FTP service in the version of Microsoft IIS 7.0 or 7.5 on the remote Windows host is affected by a command injection vulnerability that could result in unauthorized information disclosure.

### See Also

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-073>

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS Base Score

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

### CVSS Temporal Score

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

### STIG Severity

I

### References

BID	56440
-----	-------

CVE	CVE-2012-2532
MSKB	2716513
MSKB	2719033
XREF	MSFT:MS12-073
XREF	IAVB:2012-B-0111

### Plugin Information

---

Published: 2012/11/16, Modified: 2018/11/15

### Plugin Output

---

tcp/21

## 90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

### Synopsis

---

The remote Windows host is affected by an elevation of privilege vulnerability.

### Description

---

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

### See Also

---

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2016/ms16-047>

<http://badlock.org/>

### Solution

---

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

### Risk Factor

---

Medium

### CVSS Base Score

---

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

### CVSS Temporal Score

---

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

### STIG Severity

---

I

### References

---

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090

MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

### Plugin Information

---

Published: 2016/04/13, Modified: 2018/11/15

### Plugin Output

---

tcp/49157

## 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/help/887429/overview-of-server-message-block-signing>

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

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

<https://www.samba.org/samba/docs/current/man-html/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 v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

## CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

## 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: 2018/11/15

## Plugin Output

---

tcp/445

## 34324 - FTP Supports Cleartext Authentication

### Synopsis

Authentication credentials might be intercepted.

### Description

The remote FTP server allows the user's name and password to be transmitted in cleartext, which could be intercepted by a network sniffer or a man-in-the-middle attack.

### Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

### Risk Factor

Low

### CVSS Base Score

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

### References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:928
XREF	CWE:930

### Plugin Information

Published: 2008/10/01, Modified: 2016/12/08

### Plugin Output

tcp/21

```
This FTP server does not support 'AUTH TLS'.
```

### 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

### Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_7:::enterprise
```

```
Following application CPE matched on the remote system :
```

```
cpe:/a:openbsd:openssh:6.7 -> OpenBSD OpenSSH 6.7
```

### 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: 2019/05/31

### Plugin Output

tcp/135

The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91  
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, 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-2c84dalddb0d, version 1.0  
Description : Unknown RPC service  
Type : Local RPC service  
Named pipe : WMsgKRpc08C470

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 : WMsgKRpc08C470

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-c6450bee37407327b8

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 : WMsgKRpc08C691

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 : WMsgKRpc08C691

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 : Local RPC service  
Named pipe : LRPC-ac0b1bab4735ba250b

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 : Local RPC service  
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 12345778-1234-abcd- [...]

### 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: 2019/05/31

### Plugin Output

tcp/445

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91  
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
Named pipe : \PIPE\InitShutdown  
Netbios name : \\\IEWIN7

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 : \\\IEWIN7

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 : \\\IEWIN7

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 : \IEWIN7

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 : \IEWIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \IEWIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \IEWIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3cle0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \IEWIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29- [...]

```

### 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: 2019/05/31

### Plugin Output

tcp/49152

The following DCERPC services are available on TCP port 49152 :

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 10.0.0.131
```



### 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: 2019/05/31

### Plugin Output

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 : 10.0.0.131

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 : 10.0.0.131

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 : 10.0.0.131

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 : 10.0.0.131

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 : 10.0.0.131

### 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: 2019/05/31

### Plugin Output

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 : 10.0.0.131

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0  
Description : Unknown RPC service  
Annotation : IKE/Authip API  
Type : Remote RPC service  
TCP Port : 49154  
IP : 10.0.0.131

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 : 10.0.0.131

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 : 10.0.0.131

### 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: 2019/05/31

### Plugin Output

tcp/49155

The following DCERPC services are available on TCP port 49155 :

```
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 : 49155
IP : 10.0.0.131
```

### 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: 2019/05/31

### Plugin Output

tcp/49156

The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0  
Description : Unknown RPC service  
Annotation : Remote Fw APIs  
Type : Remote RPC service  
TCP Port : 49156  
IP : 10.0.0.131

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0  
Description : IPsec Services (Windows XP & 2003)  
Windows process : lsass.exe  
Annotation : IPSec Policy agent endpoint  
Type : Remote RPC service  
TCP Port : 49156  
IP : 10.0.0.131

### 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: 2019/05/31

### Plugin Output

tcp/49157

The following DCERPC services are available on TCP port 49157 :

```
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 : 49157
IP : 10.0.0.131
```

### 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

tcp/0

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



### 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

<https://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: 2018/11/15

### Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:0C:29:43:01:3E : VMware, Inc.
```

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/10/16, Modified: 2018/08/13

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:0C:29:43:01:3E
```

### Synopsis

An FTP server is listening on a remote port.

### Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2018/10/02

### Plugin Output

tcp/21

```
The remote FTP banner is :  
  
220 Microsoft FTP Service
```

## 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	CWE:200

### Plugin Information

Published: 1999/08/01, Modified: 2019/03/06

### Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -672 seconds.
```

## 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

---

<https://support.microsoft.com/en-us/help/143474/restricting-information-available-to-anonymous-logon-users>

<https://support.microsoft.com/en-us/help/246261>

### Solution

---

n/a

### Risk Factor

---

None

### Plugin Information

---

Published: 2000/05/09, Modified: 2018/11/15

### Plugin Output

---

tcp/445

- ```
- NULL sessions are enabled on the remote host.  
- Remote users are authenticated as 'Guest'.
```

### 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

---

tcp/445

```
The remote Operating System is : Windows 7 Enterprise 7600  
The remote native LAN manager is : Windows 7 Enterprise 6.1  
The remote SMB Domain Name is : IEWIN7
```

### 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

---

tcp/139

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

### 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

tcp/445

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



### Synopsis

It is possible to enumerate remote network shares.

### Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/05/09, Modified: 2018/05/16

### Plugin Output

tcp/445

```
Here are the SMB shares available on the remote host when logged in as Nessus1391938881:
```

- ADMIN\$
- C\$
- IPC\$
- shared
- Users

### 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

---

tcp/445

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

### Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

### Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/02/09, Modified: 2018/09/12

### Plugin Output

tcp/445

```
The remote host supports the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.0         Windows 8
 3.0.2       Windows 8.1
 3.1         Windows 10
 3.1.1       Windows 10
```

### 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

---

Published: 2009/02/04, Modified: 2019/06/17

### Plugin Output

---

tcp/21

```
Port 21/tcp was found to be open
```

### 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

---

Published: 2009/02/04, Modified: 2019/06/17

### Plugin Output

---

tcp/22

```
Port 22/tcp was found to be open
```

### 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

---

Published: 2009/02/04, Modified: 2019/06/17

### Plugin Output

---

tcp/135

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

### 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

---

Published: 2009/02/04, Modified: 2019/06/17

### Plugin Output

---

tcp/139

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

### 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

---

Published: 2009/02/04, Modified: 2019/06/17

### Plugin Output

---

tcp/445

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



### 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: 2019/03/06

### Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 8.3.0  
Plugin feed version : 201907082343  
Scanner edition used : Nessus Home  
Scan type : Normal  
Scan policy used : ADVANCED_NG  
Scanner IP : 10.0.0.130  
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 : enabled
Web application tests : enabled
Web app tests - Test mode : some_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/7/10 8:43 EDT
Scan duration : 234 sec
```

### 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: 2019/05/08

### Plugin Output

---

tcp/0

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

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

### 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

---

Published: 2013/07/08, Modified: 2019/06/26

### Plugin Output

---

tcp/0

```
. You need to take the following action :  
  
[ MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829)  
  (uncredentialed check) (62940) ]  
  
+ Action to take : Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.
```

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

### Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ecdsa-sha2-nistp521
ssh-dss
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
```

```
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
zlib@openssh.com
```

The server supports the following options for `compression_algorithms_server_to_client` :

```
none
zlib@openssh.com
```

## 10881 - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/03/06, Modified: 2019/05/28

### Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

## 10267 - SSH Server Type and Version Information

### Synopsis

---

An SSH server is listening on this port.

### Description

---

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

---

n/a

### Risk Factor

---

None

### Plugin Information

---

Published: 1999/10/12, Modified: 2019/01/08

### Plugin Output

---

tcp/22

```
SSH version : SSH-2.0-OpenSSH_6.7  
SSH supported authentication : publickey,password,keyboard-interactive
```



### 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/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and>

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

<http://www.nessus.org/u?234f8ef8>

<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

### Plugin Information

Published: 2017/02/03, Modified: 2018/11/15

### Plugin Output

tcp/445

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

### 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: 2019/06/25

### Plugin Output

---

tcp/21

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

### 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: 2019/06/25

### Plugin Output

---

tcp/22

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

### 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: 2019/03/06

### Plugin Output

---

tcp/0

### 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: 2019/03/06

### Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.0.130 to 10.0.0.131 :  
10.0.0.130  
10.0.0.131  
  
Hop Count: 1
```

### 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: 2019/05/31

### Plugin Output

udp/137

The following 4 NetBIOS names have been gathered :

|           |                             |
|-----------|-----------------------------|
| IEWIN7    | = File Server Service       |
| IEWIN7    | = Computer name             |
| WORKGROUP | = Workgroup / Domain name   |
| WORKGROUP | = Browser Service Elections |

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

00:0c:29:43:01:3e

---

## Remediations

---

---

## Suggested Remediations

---

Taking the following actions across 1 hosts would resolve 7% of the vulnerabilities on the network.

| ACTION TO TAKE                                                                                                                                                                               | VULNS | HOSTS |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|
| MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829)<br>(unauthenticated check): Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2. | 1     | 1     |