Nessus™

Nessus Scan Report

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

Table Of Contents

Vulnerabilities By Plugin

Remediations

Vulnerabilities By Plugin

[-] Collapse All

[+] Expand All

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

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

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

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

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

See Also

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

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

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

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

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

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

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

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

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

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

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

Solution

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

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later

SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

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

XREF	OSVDB:153678
XREF	OSVDB:153677
XREF	OSVDB:153676
XREF	OSVDB:153675
XREF	OSVDB:153674
XREF	OSVDB:153673

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

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

Hosts

192.168.15.112 (tcp/445)

192.168.15.113 (tcp/445)

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

XREF	MSFT:MS11-030
XREF	IAVA:2011-A-0039
XREF	OSVDB:71780

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/04/21, Modification date: 2014/08/29

Hosts

192.168.15.113 (udp/5355)

79638 (1) - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

See Also

https://technet.microsoft.com/library/security/ms14-066

Solution

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 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

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

References

BID	70954
CVE	CVE-2014-6321
XREF	MSFT:MS14-066
XREF	CERT:505120
XREF	OSVDB:114506

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/12/01, Modification date: 2017/06/29

Hosts

192.168.15.112 (tcp/3389)

93194 (2) - OpenSSH < 7.3 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.3. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists that is due to the program returning shorter response times for authentication requests with overly long passwords for invalid users than for valid users. This may allow a remote attacker to conduct a timing attack and enumerate valid usernames. (CVE-2016-6210)

- A denial of service vulnerability exists in the auth_password() function in auth-passwd.c due to a failure to limit password lengths for password authentication. An unauthenticated, remote attacker can exploit this, via a long string, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2016-6515)

- An unspecified flaw exists in the CBC padding oracle countermeasures that allows an unauthenticated, remote attacker to conduct a timing attack. (VulnDB 142343)

- A flaw exists due to improper operation ordering of MAC verification for Encrypt-then-MAC (EtM) mode transport MAC algorithms when verifying the MAC before decrypting any ciphertext. An unauthenticated, remote attacker can exploit this, via a timing attack, to disclose sensitive information. (VulnDB 142344)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.openssh.com/txt/release-7.3

https://marc.info/?l=openbsd-announce&m=147005433429403

Solution

Upgrade to OpenSSH version 7.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.9 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

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

CVSS Temporal Score

6.4 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	92212
CVE	CVE-2016-6210
CVE	CVE-2016-6515
XREF	OSVDB:142344
XREF	OSVDB:142343
XREF	OSVDB:142342
XREF	OSVDB:141586

Plugin Information:

Publication date: 2016/08/29, Modification date: 2016/12/07

Hosts

192.168.15.72 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_7.2
Installed version : 7.2
Fixed version : 7.3
```

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.3
```

73079 (1) - OpenSSH < 6.6 Multiple Vulnerabilities

Synopsis

The SSH server on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 6.6. It is, therefore, affected by the following vulnerabilities :

- A flaw exists due to a failure to initialize certain data structures when makefile.inc is modified to enable the J-PAKE protocol. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition and potentially the execution of arbitrary code. (CVE-2014-1692)

- An error exists related to the 'AcceptEnv' configuration setting in sshd_config due to improper processing of wildcard characters. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to bypass intended environment restrictions.
(CVE-2014-2532)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.openssh.com/txt/release-6.6

http://www.gossamer-threads.com/lists/openssh/dev/57663#57663

Solution

Upgrade to OpenSSH version 6.6 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	66355
BID	65230
CVE	CVE-2014-2532
CVE	CVE-2014-1692
XREF	OSVDB:104578
XREF	OSVDB:102611

Plugin Information:

Publication date: 2014/03/18, Modification date: 2016/06/15

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.6
```

84638 (1) - OpenSSH < 6.9 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 6.9. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the x11_open_helper() function in the 'channels.c' file that allows connections to be permitted after 'ForwardX11Timeout' has expired. A remote attacker can exploit this to bypass timeout checks and XSECURITY restrictions. (CVE-2015-5352)

- Various issues were addressed by fixing the weakness in agent locking by increasing the failure delay, storing the salted hash of the password, and using a timing-safe comparison function.

- An out-of-bounds read error exists when handling incorrect pattern lengths. A remote attacker can exploit this to cause a denial of service or disclose sensitive information in the memory.

- An out-of-bounds read error exists when parsing the 'EscapeChar' configuration option.

See Also

http://www.openssh.com/txt/release-6.9

http://www.nessus.org/u?725c4682

Solution

Upgrade to OpenSSH 6.9 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	75525
CVE	CVE-2015-5352
XREF	OSVDB:124019
XREF	OSVDB:124008

Plugin Information:

Publication date: 2015/07/09, Modification date: 2015/07/10

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.9
```

85382 (1) - OpenSSH < 7.0 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.0. It is, therefore, affected by the following vulnerabilities :

- A security bypass vulnerability exists in the kbdint_next_device() function in file auth2-chall.c that allows the circumvention of MaxAuthTries during keyboard-interactive authentication. A remote attacker can exploit this issue to force the same authentication method to be tried thousands of times in a single pass by using a crafted keyboard-interactive 'devices' string, thus allowing a brute-force attack or causing a denial of service. (CVE-2015-5600)

- A security bypass vulnerability exists in sshd due to improper handling of username data in MONITOR_REQ_PAM_INIT_CTX requests. A local attacker can exploit this, by sending a MONITOR_REQ_PWNAM request, to conduct an impersonation attack. Note that this issue only affects Portable OpenSSH. (CVE-2015-6563)

- A privilege escalation vulnerability exists due to a use-after-free error in sshd that is triggered when handling a MONITOR_REQ_PAM_FREE_CTX request. A local attacker can exploit this to gain elevated privileges.
Note that this issue only affects Portable OpenSSH.
(CVE-2015-6564)

- A local command execution vulnerability exists in sshd due to setting insecure world-writable permissions for TTYs. A local attacker can exploit this, by injecting crafted terminal escape sequences, to execute commands for logged-in users. (CVE-2015-6565)

See Also

http://www.openssh.com/txt/release-7.0

Solution

Upgrade to OpenSSH 7.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.6 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

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

CVSS Temporal Score

7.0 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	76497
BID	76317
BID	75990
CVE	CVE-2015-6565
CVE	CVE-2015-6564
CVE	CVE-2015-6563
CVE	CVE-2015-5600
XREF	EDB-ID:41173
XREF	OSVDB:126033
XREF	OSVDB:126031
XREF	OSVDB:126030

XREF	OSVDB:124938

Plugin Information:

Publication date: 2015/08/13, Modification date: 2017/04/05

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.0
```

51192 (3) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Publication date: 2010/12/15, Modification date: 2017/05/18

Hosts

192.168.15.43 (tcp/9090)

```

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=5a4fa85e0277478f8c474a86c65f8daf/CN=fedora25.localhos
t.local
|-Issuer : O=5a4fa85e0277478f8c474a86c65f8daf/CN=fedora25.localhos
t.local
```

192.168.15.112 (tcp/3389)

```

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=win81-qa-agent.localhost.local
|-Issuer : CN=win81-qa-agent.localhost.local
```

192.168.15.113 (tcp/3389)

```

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=2K8-QA-AGENT.localhost.local
|-Issuer : CN=2K8-QA-AGENT.localhost.local
```

57582 (3) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/17, Modification date: 2016/12/14

Hosts

192.168.15.43 (tcp/9090)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=5a4fa85e0277478f8c474a86c65f8daf/CN=fedora25.localhos
t.local
```

192.168.15.112 (tcp/3389)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=win81-qa-agent.localhost.local
```

192.168.15.113 (tcp/3389)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=2K8-QA-AGENT.localhost.local
```

99359 (3) - OpenSSH < 7.5

Synopsis

The SSH server running on the remote host is affected by an information disclosure vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.5. It is, therefore, affected by an information disclosure vulnerability :

- An unspecified timing flaw exists in the CBC padding oracle countermeasures, within the ssh and sshd functions, that allows an unauthenticated, remote attacker to disclose potentially sensitive information.
Note that the OpenSSH client disables CBC ciphers by default. However, sshd offers them as lowest-preference options, which will be removed by default in a future release. (VulnDB 144000)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.openssh.com/txt/release-7.5

Solution

Upgrade to OpenSSH version 7.5 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (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)

References

XREF	OSVDB:144000

Plugin Information:

Publication date: 2017/04/13, Modification date: 2017/04/17

Hosts

192.168.15.43 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_7.4
Installed version : 7.4
Fixed version : 7.5
```

192.168.15.72 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_7.2
Installed version : 7.2
Fixed version : 7.5
```

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.5
```

35291 (2) - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	33065
BID	11849
CVE	CVE-2004-2761
XREF	CWE:310
XREF	CERT:836068
XREF	OSVDB:45127
XREF	OSVDB:45108
XREF	OSVDB:45106

Plugin Information:

Publication date: 2009/01/05, Modification date: 2017/06/12

Hosts

192.168.15.112 (tcp/3389)

```

The following certificates were part of the certificate chain sent
by
the remote host, but contain hashes that are considered to be weak.

|-Subject : CN=win81-qa-agent.localhost.local
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : May 15 21:36:18 2017 GMT
|-Valid To : Nov 14 21:36:18 2017 GMT
```

192.168.15.113 (tcp/3389)

```

The following certificates were part of the certificate chain sent
by
the remote host, but contain hashes that are considered to be weak.

|-Subject : CN=2K8-QA-AGENT.localhost.local
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : May 15 21:07:47 2017 GMT
|-Valid To : Nov 14 21:07:47 2017 GMT
```

42873 (2) - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

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)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2017/06/29

Hosts

192.168.15.112 (tcp/3389)

```
Here is the list of medium strength SSL ciphers supported by the re
mote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

TLSv11
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

TLSv12
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.113 (tcp/3389)

```
Here is the list of medium strength SSL ciphers supported by the re
mote server :
```

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

57608 (2) - 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: 2016/12/09

Hosts

192.168.15.112 (tcp/445)

192.168.15.113 (tcp/445)

90023 (2) - OpenSSH < 7.2p2 X11Forwarding xauth Command Injection

Synopsis

The SSH server running on the remote host is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.2p2. It is, therefore, affected by a security bypass vulnerability due to improper sanitization of X11 authentication credentials. An authenticated, remote attacker can exploit this, via crafted credentials, to inject arbitrary xauth commands, resulting in gaining read and write access to arbitrary files, connecting to local ports, or performing further attacks on xauth itself. Note that exploiting this vulnerability requires X11Forwarding to have been enabled.

See Also

http://www.openssh.com/txt/release-7.2p2

http://www.openssh.com/txt/x11fwd.adv

Solution

Upgrade to OpenSSH version 7.2p2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.0 (CVSS2#E:F/RL:OF/RC:ND)

References

CVE	CVE-2016-3115
XREF	EDB-ID:39569
XREF	OSVDB:135714

Plugin Information:

Publication date: 2016/03/18, Modification date: 2016/09/01

Hosts

192.168.15.72 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_7.2
Installed version : 7.2
Fixed version : 7.2p2
```

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.2p2
```

90510 (2) - 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://technet.microsoft.com/library/security/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

5.6 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
XREF	IAVA:2016-A-0093
XREF	CERT:813296
XREF	MSFT:MS16-047
XREF	OSVDB:136339

Plugin Information:

Publication date: 2016/04/13, Modification date: 2016/07/19

Hosts

192.168.15.112 (tcp/49154)

192.168.15.113 (tcp/49193)

94437 (2) - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

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

5.1 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92631
BID	92630
CVE	CVE-2016-6329
CVE	CVE-2016-2183
XREF	OSVDB:143388
XREF	OSVDB:143387

Plugin Information:

Publication date: 2016/11/01, Modification date: 2017/01/24

Hosts

192.168.15.112 (tcp/3389)

```
List of 64-bit block cipher suites supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
```

```
The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.113 (tcp/3389)

```
List of 64-bit block cipher suites supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

96151 (2) - OpenSSH < 7.4 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.4. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in ssh-agent due to loading PKCS#11 modules from paths that are outside a trusted whitelist.
A local attacker can exploit this, by using a crafted request to load hostile modules via agent forwarding, to execute arbitrary code. To exploit this vulnerability, the attacker would need to control the forwarded agent-socket (on the host running the sshd server) and the ability to write to the file system of the host running ssh-agent. (CVE-2016-10009)

- A flaw exists in sshd due to creating forwarded Unix-domain sockets with 'root' privileges whenever privilege separation is disabled. A local attacker can exploit this to gain elevated privileges.
(CVE-2016-10010)

- An information disclosure vulnerability exists in sshd within the realloc() function due leakage of key material to privilege-separated child processes when reading keys. A local attacker can possibly exploit this to disclose sensitive key material. Note that no such leak has been observed in practice for normal-sized keys, nor does a leak to the child processes directly expose key material to unprivileged users.
(CVE-2016-10011)

- A flaw exists in sshd within the shared memory manager used by pre-authenticating compression support due to a bounds check being elided by some optimizing compilers and due to the memory manager being incorrectly accessible when pre-authenticating compression is disabled. A local attacker can exploit this to gain elevated privileges. (CVE-2016-10012)

- A denial of service vulnerability exists in sshd when handling KEXINIT messages. An unauthenticated, remote attacker can exploit this, by sending multiple KEXINIT messages, to consume up to 128MB per connection.
(VulnDB 148976)

- A flaw exists in sshd due to improper validation of address ranges by the AllowUser and DenyUsers directives at configuration load time. A local attacker can exploit this, via an invalid CIDR address range, to gain access to restricted areas. (VulnDB 148977)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.openssh.com/txt/release-7.4

Solution

Upgrade to OpenSSH version 7.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

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

CVSS Temporal Score

5.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	94977
BID	94975
BID	94972
BID	94968
CVE	CVE-2016-10012
CVE	CVE-2016-10011
CVE	CVE-2016-10010
CVE	CVE-2016-10009
XREF	EDB-ID:40962
XREF	OSVDB:148977
XREF	OSVDB:148976

XREF	OSVDB:148975
XREF	OSVDB:148968
XREF	OSVDB:148967
XREF	OSVDB:148966

Plugin Information:

Publication date: 2016/12/27, Modification date: 2016/12/29

Hosts

192.168.15.72 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_7.2
Installed version : 7.2
Fixed version : 7.4
```

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.4
```

44081 (1) - OpenSSH < 5.7 Multiple Vulnerabilities

Synopsis

The remote SSH service may be affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.7. Versions before 5.7 may be affected by the following vulnerabilities :

- A security bypass vulnerability because OpenSSH does not properly validate the public parameters in the J-PAKE protocol. This could allow an attacker to authenticate without the shared secret. Note that this issue is only exploitable when OpenSSH is built with J-PAKE support, which is currently experimental and disabled by default, and that Nessus has not checked whether J-PAKE support is indeed enabled. (CVE-2010-4478)

- The auth_parse_options function in auth-options.c in sshd provides debug messages containing authorized_keys command options, which allows remote, authenticated users to obtain potentially sensitive information by reading these messages. (CVE-2012-0814)

See Also

http://seb.dbzteam.org/crypto/jpake-session-key-retrieval.pdf

http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c#rev1.5

http://www.nessus.org/u?3f1722f0

Solution

Upgrade to OpenSSH 5.7 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	51702
BID	45304
CVE	CVE-2012-0814
CVE	CVE-2010-4478
XREF	OSVDB:78706
XREF	OSVDB:69658

Plugin Information:

Publication date: 2011/10/04, Modification date: 2016/12/07

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 5.7
```

67140 (1) - OpenSSH LoginGraceTime / MaxStartups DoS

Synopsis

The remote SSH service is susceptible to a remote denial of service attack.

Description

According to its banner, a version of OpenSSH earlier than version 6.2 is listening on this port. The default configuration of OpenSSH installs before 6.2 could allow a remote attacker to bypass the LoginGraceTime and MaxStartups thresholds by periodically making a large number of new TCP connections and thereby prevent legitimate users from gaining access to the service.

Note that this plugin has not tried to exploit the issue or detect whether the remote service uses a vulnerable configuration. Instead, it has simply checked the version of OpenSSH running on the remote host.

See Also

http://www.openwall.com/lists/oss-security/2013/02/06/5

http://openssh.org/txt/release-6.2

https://tools.cisco.com/security/center/viewAlert.x?alertId=28883

Solution

Upgrade to OpenSSH 6.2 and review the associated server configuration settings.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	58162
CVE	CVE-2010-5107
XREF	OSVDB:90007

Plugin Information:

Publication date: 2013/07/03, Modification date: 2017/06/12

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.2
```

90022 (1) - OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass

Synopsis

The SSH server running on the remote host is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.2. It is, therefore, affected by a security bypass vulnerability due to a flaw in ssh(1) that is triggered when it falls back from untrusted X11 forwarding to trusted forwarding when the SECURITY extension is disabled by the X server. This can result in untrusted X11 connections that can be exploited by a remote attacker.

See Also

http://www.openssh.com/txt/release-7.2

Solution

Upgrade to OpenSSH version 7.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

XREF	OSVDB:135128

Plugin Information:

Publication date: 2016/03/18, Modification date: 2016/04/28

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.2
```

90317 (1) - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

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: 2016/04/04, Modification date: 2016/12/14

Hosts

192.168.15.85 (tcp/22)

```
The following weak server-to-client encryption algorithms are suppo
rted :

arcfour
arcfour128
arcfour256

The following weak client-to-server encryption algorithms are suppo
rted :

arcfour
arcfour128
arcfour256
```

65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	73684
BID	58796
CVE	CVE-2015-2808
CVE	CVE-2013-2566
XREF	OSVDB:117855
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2016/12/14

Hosts

192.168.15.112 (tcp/3389)

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.113 (tcp/3389)

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

53841 (1) - Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure

Synopsis

Local attackers may be able to access sensitive information.

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.8p2. Such versions may be affected by a local information disclosure vulnerability that could allow the contents of the host's private key to be accessible by locally tracing the execution of the ssh-keysign utility. Having the host's private key may allow the impersonation of the host.

Note that installations are only vulnerable if ssh-rand-helper was enabled during the build process, which is not the case for *BSD, OS X, Cygwin and Linux.

See Also

http://www.openssh.com/txt/portable-keysign-rand-helper.adv

http://www.openssh.com/txt/release-5.8p2

Solution

Upgrade to Portable OpenSSH 5.8p2 or later.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	47691
CVE	CVE-2011-4327
XREF	Secunia:44347
XREF	OSVDB:72183

Plugin Information:

Publication date: 2011/05/09, Modification date: 2016/12/07

Hosts

192.168.15.85 (tcp/22)

```
Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 5.8p2
```

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	CWE:200
XREF	CERT:958563
XREF	OSVDB:50036
XREF	OSVDB:50035

Plugin Information:

Publication date: 2013/10/28, Modification date: 2016/05/12

Hosts

192.168.15.85 (tcp/22)

```
The following client-to-server Cipher Block Chaining (CBC) algorith
ms
are supported :
```

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorith
ms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

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: 2013/11/22, Modification date: 2016/12/14

Hosts

192.168.15.85 (tcp/22)

```
The following client-to-server Message Authentication Code (MAC) al
gorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) al
gorithms
are supported :

hmac-md5
```

```
hmac-md5-96
hmac-sha1-96
```

86328 (1) - SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSH connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote SSH server allows connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time (depending on modulus size and attacker resources).
This allows an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

http://weakdh.org/

https://stribika.github.io/2015/01/04/secure-secure-shell.html

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS Base Score

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

References

BID	74733
CVE	CVE-2015-4000
XREF	OSVDB:122331

Plugin Information:

Publication date: 2015/10/09, Modification date: 2017/05/30

Hosts

192.168.15.85 (tcp/22)

```
The SSH server is vulnerable to the Logjam attack because :

It supports diffie-hellman-group1-sha1 key
exchange.

It supports diffie-hellman-group-exchange-sha1
key exchange and allows a moduli smaller than
or equal to 1024.

Note that only an attacker with nation-state level resources
can effectively make use of the vulnerability, and only
against sessions where the vulnerable key exchange
algorithms are used.
```

11219 (30) - 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: 2017/05/22

Hosts

192.168.15.43 (tcp/22)

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

192.168.15.43 (tcp/9090)

```
Port 9090/tcp was found to be open
```

192.168.15.72 (tcp/22)

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

192.168.15.85 (tcp/22)

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

192.168.15.112 (tcp/135)

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

192.168.15.112 (tcp/139)

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

192.168.15.112 (tcp/445)

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

192.168.15.112 (tcp/554)

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

192.168.15.112 (tcp/2869)

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

192.168.15.112 (tcp/3389)

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

192.168.15.112 (tcp/10243)

```
Port 10243/tcp was found to be open
```

192.168.15.112 (tcp/49152)

```
Port 49152/tcp was found to be open
```

192.168.15.112 (tcp/49153)

```
Port 49153/tcp was found to be open
```

192.168.15.112 (tcp/49154)

```
Port 49154/tcp was found to be open
```

192.168.15.112 (tcp/49155)

```
Port 49155/tcp was found to be open
```

192.168.15.112 (tcp/49156)

```
Port 49156/tcp was found to be open
```

192.168.15.112 (tcp/49157)

```
Port 49157/tcp was found to be open
```

192.168.15.112 (tcp/49179)

```
Port 49179/tcp was found to be open
```

192.168.15.112 (tcp/49188)

```
Port 49188/tcp was found to be open
```

192.168.15.113 (tcp/135)

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

192.168.15.113 (tcp/139)

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

192.168.15.113 (tcp/445)

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

192.168.15.113 (tcp/3389)

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

192.168.15.113 (tcp/47001)

```
Port 47001/tcp was found to be open
```

192.168.15.113 (tcp/49152)

```
Port 49152/tcp was found to be open
```

192.168.15.113 (tcp/49153)

```
Port 49153/tcp was found to be open
```

192.168.15.113 (tcp/49154)

```
Port 49154/tcp was found to be open
```

192.168.15.113 (tcp/49183)

```
Port 49183/tcp was found to be open
```

192.168.15.113 (tcp/49190)

```
Port 49190/tcp was found to be open
```

192.168.15.113 (tcp/49193)

```
Port 49193/tcp was found to be open
```

10736 (18) - 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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Hosts

192.168.15.112 (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 : WMsgKRpc048680

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 : WMsgKRpc048680

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : OLEC89349494308C1332B8E556BAE50

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : dabrpc

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : LRPC-72f72f3731ea906227

    Object UUID : b08669ee-8cb5-43a5-a017-84fe00000002
    UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : WMsgKRpc044FA252

    Object UUID : 52ef130c-08fd-4388-86b3-6edf00000002
    UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
    Description : Unknown RPC service
    Annotation : Secure Desktop LRPC interface
    Type : Local RPC service
    Named pipe : WMsgKRpc044FA252

    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-f91d7b6ca7cc0b204e

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : LRPC-f91d7b6ca7cc0b204e

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : OLE7B5C7AD96A88222A42BB749B4F56

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
    Description : Unknown RPC service
    Type : Local RPC service
    Named pipe : LRPC-5f9413794e99d87238

    Object UUID : 00000000-0000-0000-0000-000000000000
    UUID : c100beac-d33a-4a4b-bf23-bbef4663d017, version 1.0
    Description : Unknown RPC service
    Annotation : wcncsvc.transport
    Type : Local RPC service
```

```
Named pipe : LRPC-f91d7b6ca7cc0b204e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beac-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.transport
Type : Local RPC service
Named pipe : OLE7B5C7AD96A88222A42BB749B4F56

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beac-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.transport
Type : Local RPC service
Named pipe : LRPC-5f9413794e99d87238

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beac-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.transport
Type : Local RPC service
Named pipe : wcncsvc.transport

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : LRPC-f91d7b6ca7cc0b204e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : OLE7B5C7AD96A88222A42BB749B4F56

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : LRPC-5f9413794e99d87238

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : wcncsvc.transport

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : wcncsvc.wcnprpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f763c91c-2ab1-47fa-868f-7de7efd42194, version 1.0
Description : Unknown RPC service
Annotation : VM Allow-List Provider RPC
Type : Local RPC service
Named pipe : OLE26DF96213E1C80BE620D4C43622F
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f763c91c-2ab1-47fa-868f-7de7efd42194, version 1.0
Description : Unknown RPC service
Annotation : VM Allow-List Provider RPC
Type : Local RPC service
Named pipe : RdvVmAllowListRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-726107460c8af48012

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-726107460c8af48012

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE80200310EF75E95ADCD95D94B784

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : RemoteDevicesLPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : TSUMRPD_PRINT_DRV_LPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
Type : Local RPC service
Named pipe : LRPC-726107460c8af48012

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
Type : Local RPC service
Named pipe : trkwks

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
```

```
Type : Local RPC service
Named pipe : OLE80200310EF75E95ADCD95D94B784

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
Type : Local RPC service
Named pipe : RemoteDevicesLPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
Type : Local RPC service
Named pipe : TSUMRPD_PRINT_DRV_LPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-726107460c8af48012

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : trkwks

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : OLE80200310EF75E95ADCD95D94B784

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : RemoteDevicesLPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : TSUMRPD_PRINT_DRV_LPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : LRPC-726107460c8af48012

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
```

```
Type : Local RPC service
Named pipe : trkwks

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : OLE80200310EF75E95ADCD95D94B784

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : RemoteDevicesLPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : TSUMRPD_PRINT_DRV_LPC_API

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2c9b409-c1c9-4100-8639-d8ab1486694a, version 1.0
Description : Unknown RPC service
Annotation : Witness Client Upcall Server
Type : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2c9b409-c1c9-4100-8639-d8ab1486694a, version 1.0
Description : Unknown RPC service
Annotation : Witness Client Upcall Server
Type : Local RPC service
Named pipe : LRPC-769340de8df3257b2b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : eb081a0d-10ee-478a-a1dd-50995283e7a8, version 3.0
Description : Unknown RPC service
Annotation : Witness Client Test Interface
Type : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : eb081a0d-10ee-478a-a1dd-50995283e7a8, version 3.0
Description : Unknown RPC service
Annotation : Witness Client Test Interface
Type : Local RPC service
Named pipe : LRPC-769340de8df3257b2b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Local RPC service
Named pipe : LRPC-769340de8df3257b2b
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-769340de8df3257b2b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : keysvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECAE1771716C198B7B1DCB01A610D

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlaplg

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlaapi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-946b2960dba4f8aea2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-946b2960dba4f8aea2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-62508cc321d4a3628a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-946b2960dba4f8aea2
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-62508cc321d4a3628a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-946b2960dba4f8aea2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-62508cc321d4a3628a

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000001
UUID : b2507c30-b126-494a-92ac-ee32b6eeb039, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b816e213fd7c09aa00

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
Type : Local RPC service
Named pipe : LRPC-61b16f3665bf7689ef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-61b16f3665bf7689ef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-61b16f3665bf7689ef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-61b16f3665bf7689ef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-61b16f3665bf7689ef

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-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

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 : LSARPC_ENDPOINT

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 : lsacap

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 : LSA_IDPEXT_ENDPOINT

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 : LSA_EAS_ENDPOINT

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 : lsapolicylookup

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 : lsasspirpc

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 : protected_storage

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 : SidKey Local End Point

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 : samss lpc

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : audit

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : securityevent

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsacap

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
```

```
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : NETLOGON_LRPC

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : audit

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : securityevent

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsacap

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT
```

```
Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Local RPC service
Named pipe : NETLOGON_LRPC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLEF343ED4FA8CF64B5589DDA8C4E5C

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-439090f1a63d736a32

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : OLEF343ED4FA8CF64B5589DDA8C4E5C

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-439090f1a63d736a32

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : W32TIME_ALT

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
```

```
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
```

```
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

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 : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

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 : Local RPC service
Named pipe : IUserProfile2

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 : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

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 : Local RPC service
Named pipe : senssvc

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 : Local RPC service
Named pipe : ubpmtaskhostchannel

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 : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

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 : Local RPC service
Named pipe : IUserProfile2

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 : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

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 : Local RPC service
```

```
Named pipe : senssvc

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 : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
```

```
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e94d7f9d0c061f6cb6

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-99921c81ced29eda1b

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLE5FB4E14888621B049FAA133CB015

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
```

```
Named pipe : LRPC-e94d7f9d0c061f6cb6

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : AudioClientRpc

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 : Local RPC service
Named pipe : Audiosrv

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 : Local RPC service
Named pipe : PlaybackManagerRpc

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : AudioClientRpc

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 : Local RPC service
Named pipe : Audiosrv

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 : Local RPC service
Named pipe : PlaybackManagerRpc
```

```
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 : Local RPC service
Named pipe : dhcpcsvc6

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : AudioClientRpc

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 : Local RPC service
Named pipe : Audiosrv

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 : Local RPC service
Named pipe : PlaybackManagerRpc

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 : Local RPC service
Named pipe : dhcpcsvc6

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 : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
```

```
Annotation : Wcm Service
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Local RPC service
Named pipe : PlaybackManagerRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : PlaybackManagerRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
```

```
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLE322619993020EC275E3D2B0B6D42

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 : WMsgKRpc04AF11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 085b0334-e454-4d91-9b8c-4134f9e793f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 085b0334-e454-4d91-9b8c-4134f9e793f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8782d3b9-ebbd-4644-a3d8-e8725381919b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8782d3b9-ebbd-4644-a3d8-e8725381919b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3b338d89-6cfa-44b8-847e-531531bc9992, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3b338d89-6cfa-44b8-847e-531531bc9992, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

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 : umpo

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 : actkernel

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-6d821aaeb93400ae18

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6d821aaeb93400ae18

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LSMApi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-72f72f3731ea906227

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6d821aaeb93400ae18

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LSMApi
```

192.168.15.112 (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 : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Rese
t module
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\WIN81-QA-AGENT
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\WIN81-QA-AGENT

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

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 : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

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
```

```
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN81-QA-AGENT

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT
```

```
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
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\LSM_API_service
Netbios name : \\WIN81-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\LSM_API_service
Netbios name : \\WIN81-QA-AGENT
```

192.168.15.112 (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 : 192.168.15.112
```

192.168.15.112 (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 : 192.168.15.112

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 : 192.168.15.112

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 : 192.168.15.112

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 : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Annotation : Wcm Service
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.15.112

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 : 192.168.15.112
```

192.168.15.112 (tcp/49154)

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

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 : 49154
IP : 192.168.15.112

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.15.112

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
```

```
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.15.112
```

192.168.15.112 (tcp/49155)

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

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 : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

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 : 49155
IP : 192.168.15.112

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 : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

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 : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.15.112
```

192.168.15.112 (tcp/49156)

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

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
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.15.112

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
```

```
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.15.112
```

192.168.15.112 (tcp/49157)

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.15.112

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.15.112
```

192.168.15.112 (tcp/49179)

```
The following DCERPC services are available on TCP port 49179 :

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 : 49179
IP : 192.168.15.112
```

192.168.15.112 (tcp/49188)

```
The following DCERPC services are available on TCP port 49188 :

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 : 49188
IP : 192.168.15.112
```

192.168.15.113 (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 : WMsgKRpc03A290

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 : WMsgKRpc03A290

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-3bd3a84e1681cbdc2c

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 : WMsgKRpc03A501

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 : WMsgKRpc03A501

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000003
UUID : 24019106-a203-4642-b88d-82dae9158929, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cdb7a359ecf4c6ceff

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000003
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0207F13

Object UUID : 60dc6e82-dd34-4706-b4eb-21d660fc0c7e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-dee70e8f44758f907b

Object UUID : 0aa2b4b1-b29e-4095-b722-dee018925ef1
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-dee70e8f44758f907b

Object UUID : 271ccc6d-3952-42c5-b3b2-3e93a900a672
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
```

```
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-dee70e8f44758f907b

Object UUID : 0bd0f976-4aa1-4506-af44-2a07efce9a29
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-dee70e8f44758f907b

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-74cd6c7d5dc5430b7b

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-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

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 : LSARPC_ENDPOINT

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 : lsapolicylookup

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 : lsasspirpc

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 : protected_storage

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 : dsrole

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 : samss lpc

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 : Local RPC service
Named pipe : LRPC-311f8bc40b800d6035

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f763c91c-2ab1-47fa-868f-7de7efd42194, version 1.0
Description : Unknown RPC service
Annotation : VM Allow-List Provider RPC
Type : Local RPC service
Named pipe : OLEA257C2E3243941A3A0BD547FBBC4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f763c91c-2ab1-47fa-868f-7de7efd42194, version 1.0
Description : Unknown RPC service
Annotation : VM Allow-List Provider RPC
Type : Local RPC service
Named pipe : RdvVmAllowListRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-7f8db9dc9cde034235

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-7f8db9dc9cde034235

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-7f8db9dc9cde034235

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLE9D855F36B87849598FE190141A61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
```

```
Named pipe : LRPC-977c8798de3b7ff2d5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : OLE9D855F36B87849598FE190141A61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-977c8798de3b7ff2d5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : W32TIME_ALT

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 6c637067-6569-746e-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 : IUserProfile2

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
```

```
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

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 : Local RPC service
Named pipe : IUserProfile2

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 : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

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 : Local RPC service
Named pipe : senssvc

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 : Local RPC service
Named pipe : IUserProfile2

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 : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

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 : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEDBC32F35B813462784CC24246090

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
```

```
Named pipe : eventlog

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 : Local RPC service
Named pipe : dhcpcsvc

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : dhcpcsvc

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 : Local RPC service
Named pipe : dhcpcsvc6

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 : Local RPC service
Named pipe : eventlog

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 : Local RPC service
Named pipe : dhcpcsvc

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 : Local RPC service
Named pipe : dhcpcsvc6
```

192.168.15.113 (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 : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

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 : \\2K8-QA-AGENT

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
Named pipe : \PIPE\atsvc
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \PIPE\atsvc
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \PIPE\atsvc
Netbios name : \\2K8-QA-AGENT

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\2K8-QA-AGENT

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\2K8-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\2K8-QA-AGENT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \pipe\eventlog
```

```
Netbios name : \\2K8-QA-AGENT

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
Named pipe : \pipe\eventlog
Netbios name : \\2K8-QA-AGENT
```

192.168.15.113 (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 : 192.168.15.113
```

192.168.15.113 (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 : 192.168.15.113

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 : 192.168.15.113

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 : 192.168.15.113

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 : 192.168.15.113
```

192.168.15.113 (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 : 192.168.15.113

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 : 192.168.15.113

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 : 192.168.15.113

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 : 192.168.15.113

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.15.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.15.113
```

192.168.15.113 (tcp/49183)

```
The following DCERPC services are available on TCP port 49183 :

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 : 49183
IP : 192.168.15.113
```

192.168.15.113 (tcp/49190)

```
The following DCERPC services are available on TCP port 49190 :

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 : 49190
IP : 192.168.15.113

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 : 49190
IP : 192.168.15.113
```

192.168.15.113 (tcp/49193)

```
The following DCERPC services are available on TCP port 49193 :

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 : 49193
IP : 192.168.15.113
```

22964 (7) - 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: 2017/07/07

Hosts

192.168.15.43 (tcp/22)

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

192.168.15.43 (tcp/9090)

```
A TLSv1.1 server answered on this port.
```

192.168.15.43 (tcp/9090)

```
A web server is running on this port through TLSv1.1.
```

192.168.15.72 (tcp/22)

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

192.168.15.85 (tcp/22)

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

192.168.15.112 (tcp/10243)

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

192.168.15.113 (tcp/47001)

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

10114 (5) - 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
XREF	OSVDB:94

Plugin Information:

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

Hosts

192.168.15.43 (icmp/0)

```
The remote clock is synchronized with the local clock.
```

192.168.15.72 (icmp/0)

```
The remote clock is synchronized with the local clock.
```

192.168.15.85 (icmp/0)

```
The difference between the local and remote clocks is 62 seconds.
```

192.168.15.112 (icmp/0)

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in networ
k format)
The remote clock is synchronized with the local clock.
```

192.168.15.113 (icmp/0)

```
The ICMP timestamps seem to be in little endian format (not in netw
ork format)
The difference between the local and remote clocks is -124 seconds.
```

10287 (5) - 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

Hosts

192.168.15.43 (udp/0)

```
For your information, here is the traceroute from 192.168.15.108 to
192.168.15.43 :
192.168.15.108
192.168.15.43
```

192.168.15.72 (udp/0)

```
For your information, here is the traceroute from 192.168.15.108 to
192.168.15.72 :
192.168.15.108
192.168.15.72
```

192.168.15.85 (udp/0)

```
For your information, here is the traceroute from 192.168.15.108 to
192.168.15.85 :
192.168.15.108
192.168.15.85
```

192.168.15.112 (udp/0)

```
For your information, here is the traceroute from 192.168.15.108 to
192.168.15.112 :
192.168.15.108
192.168.15.112
```

192.168.15.113 (udp/0)

```
For your information, here is the traceroute from 192.168.15.108 to
192.168.15.113 :
192.168.15.108
192.168.15.113
```

12053 (5) - 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:

Publication date: 2004/02/11, Modification date: 2017/04/14

Hosts

192.168.15.43 (tcp/0)

```
192.168.15.43 resolves as fedora25.localhost.local.
```

192.168.15.72 (tcp/0)

```
192.168.15.72 resolves as suse12.localhost.local.
```

192.168.15.85 (tcp/0)

```
192.168.15.85 resolves as rhel6.localhost.local.
```

192.168.15.112 (tcp/0)

```
192.168.15.112 resolves as win81-qa-agent.localhost.local.
```

192.168.15.113 (tcp/0)

```
192.168.15.113 resolves as 2k8-qa-agent.localhost.local.
```

19506 (5) - 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: 2017/05/22

Hosts

192.168.15.43 (tcp/0)

```
Information about this scan :

Nessus version : 6.11.0
Plugin feed version : 201707121215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.15.108
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 2
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 : 2017/7/14 13:26 Eastern Standard Time
Scan duration : 1317 sec
```

192.168.15.72 (tcp/0)

```
Information about this scan :

Nessus version : 6.11.0
Plugin feed version : 201707121215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.15.108
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 2
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 : 2017/7/14 13:26 Eastern Standard Time
Scan duration : 128 sec
```

192.168.15.85 (tcp/0)

```
Information about this scan :

Nessus version : 6.11.0
Plugin feed version : 201707121215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.15.108
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 2
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 : 2017/7/14 13:26 Eastern Standard Time
Scan duration : 1101 sec
```

192.168.15.112 (tcp/0)

```
Information about this scan :

Nessus version : 6.11.0
Plugin feed version : 201707121215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.15.108
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 2
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 : 2017/7/14 13:26 Eastern Standard Time
Scan duration : 383 sec
```

192.168.15.113 (tcp/0)

```
Information about this scan :

Nessus version : 6.11.0
Plugin feed version : 201707121215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.15.108
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 2
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 : 2017/7/14 13:26 Eastern Standard Time
Scan duration : 256 sec
```

25220 (5) - 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

Hosts

192.168.15.43 (tcp/0)

192.168.15.72 (tcp/0)

192.168.15.85 (tcp/0)

192.168.15.112 (tcp/0)

192.168.15.113 (tcp/0)

35716 (5) - 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

Hosts

192.168.15.43 (tcp/0)

```

The following card manufacturers were identified :

00:15:5d:0f:c6:af : Microsoft Corporation
```

192.168.15.72 (tcp/0)

```

The following card manufacturers were identified :

00:15:5d:0f:c6:93 : Microsoft Corporation
```

192.168.15.85 (tcp/0)

```

The following card manufacturers were identified :

00:15:5d:0f:c6:b9 : Microsoft Corporation
```

192.168.15.112 (tcp/0)

```

The following card manufacturers were identified :

00:15:5d:0f:c6:aa : Microsoft Corporation
```

192.168.15.113 (tcp/0)

```

The following card manufacturers were identified :

00:15:5d:0f:c6:ab : Microsoft Corporation
```

45590 (5) - 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Hosts

192.168.15.43 (tcp/0)

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

cpe:/a:openbsd:openssh:7.4
```

192.168.15.72 (tcp/0)

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

cpe:/o:linux:linux_kernel:3.10
cpe:/o:linux:linux_kernel:3.13
cpe:/o:linux:linux_kernel:4.2
cpe:/o:linux:linux_kernel:4.8

Following application CPE matched on the remote system :

cpe:/a:openbsd:openssh:7.2
```

192.168.15.85 (tcp/0)

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

cpe:/a:openbsd:openssh:5.3 -> OpenBSD OpenSSH 5.3
```

192.168.15.112 (tcp/0)

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

cpe:/o:microsoft:windows_8_1:::enterprise
```

192.168.15.113 (tcp/0)

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

cpe:/o:microsoft:windows_server_2008:r2:sp1:enterprise
```

84047 (5) - Hyper-V Virtual Machine Detection

Synopsis

The remote host is a Hyper-V virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a Microsoft Hyper-V virtual machine.

See Also

http://www.nessus.org/u?55895693

http://www.nessus.org/u?7ef0cc51

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: 2015/06/09, Modification date: 2017/03/03

Hosts

192.168.15.43 (tcp/0)

```
The remote host is a Hyper-V virtual machine.
```

192.168.15.72 (tcp/0)

```
The remote host is a Hyper-V virtual machine.
```

192.168.15.85 (tcp/0)

```
The remote host is a Hyper-V virtual machine.
```

192.168.15.112 (tcp/0)

```
The remote host is a Hyper-V virtual machine.
```

192.168.15.113 (tcp/0)

```
The remote host is a Hyper-V virtual machine.
```

11011 (4) - 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

Hosts

192.168.15.112 (tcp/139)

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

192.168.15.112 (tcp/445)

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

192.168.15.113 (tcp/139)

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

192.168.15.113 (tcp/445)

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

10267 (3) - 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:

Publication date: 1999/10/12, Modification date: 2017/05/30

Hosts

192.168.15.43 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_7.4
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-m
ic,password
```

192.168.15.72 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_7.2
SSH supported authentication : publickey,keyboard-interactive
```

192.168.15.85 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-m
ic,password
```

10863 (3) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Hosts

192.168.15.43 (tcp/9090)

```
Subject Name:

Organization: 5a4fa85e0277478f8c474a86c65f8daf
Common Name: fedora25.localhost.local

Issuer Name:

Organization: 5a4fa85e0277478f8c474a86c65f8daf
Common Name: fedora25.localhost.local

Serial Number: 00 BD 6A 1B A2 E7 DE C2 FD

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 23 22:14:10 2017 GMT
Not Valid After: Dec 30 22:14:10 2116 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 DB DA F1 B5 67 78 01 05 62 28 49 C1 BA C6 AD B0 6
6 61
52 33 1C 5D 0A 6D A6 22 68 98 F6 C0 6B 08 6E 84 CF 62 33 84
8A 81 3E BE 73 C8 41 9C 4D B4 BD 6D 4B 01 A9 9A 06 98 A3 83
C8 39 78 49 8B BD 74 2B 08 69 86 8B B6 93 5F 34 2A 08 62 C4
31 0A 6E 58 AB B6 42 F5 C9 51 EA 0E F0 1B E4 32 8E 38 24 26
98 EE 1B B9 4E 81 81 F8 97 99 D6 F4 09 92 AC FF 33 A8 4C B2
0F 59 A0 2B E2 83 11 73 7B 41 6B D7 91 AB CE 57 89 E1 D1 47
```

```
0F 6B F6 43 B0 38 40 BC 15 E6 C0 65 91 CD 22 5E 63 78 AD 08
BA 8E C2 0F 16 EA 79 9F 8D 26 FC BD 9E AD C0 3B C4 24 F0 B3
0C 0F 2D 1E 48 E6 8E 31 DE CA 12 92 0E BB 21 62 20 36 91 57
C2 FC A1 B2 E5 33 D8 B4 55 9C AD E2 10 79 5A DB B0 7D F7 43
78 4C 9C 10 6B EF C2 13 36 CB 1F 19 CD 7B C8 F3 E2 4A 22 F2
B0 AD FE CB D1 75 FE E7 BF AF AD CC DE 44 38 47 63
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 20 13 4C B0 B9 27 91 F3 CF 9B 91 2C A0 4E BD 73 3C 7A
95
9A 4B 8D 2B 82 43 CE BA 9F 34 A7 18 5C 73 E5 95 58 69 DF 1F
2F EE 09 35 38 7A 6A 14 80 EB 22 1B 0D 2E 25 76 94 78 6C 01
88 AB BF 61 80 FD 8E 09 59 11 32 99 2E AA 8E 9A 06 43 6C CF
BE A2 A0 78 40 94 C0 2B 92 1C 2E 61 7E 21 CB 33 91 12 4A EB
82 28 9A ED 57 B9 B5 5B BA 27 45 BD FC E0 04 F6 C4 42 76 21
96 EF 81 7B 2D A2 62 3A EA DD 5D C7 84 2A 9B C1 B2 05 53 A9
4D 04 4B 82 C0 DA 3F 79 E5 4F D4 CF AC 28 D1 56 7B E9 0A E0
EA 9A 81 70 FC 20 43 30 04 E5 BA 00 43 52 64 D0 98 5D EE 6F
C6 41 BC F7 E8 6A F3 F5 B4 5B 23 2F 45 3C A3 CD E3 FD EE 3A
93 51 F3 50 C0 6D 4F DE C1 0F 11 B9 95 7A B7 75 CF 4F 1D 1B
C1 70 4C 63 00 A0 60 92 AE DC 8E 48 D6 96 DD F3 54 C8 25 DF
AA 56 84 65 5F DC CA 24 25 FF 1C DB 13 31 A4 99 29

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 0F 08 88 F5 9F B0 D9 B2 87 52 DD 4A F6 BF 0
D 5A 3D 17 34 A2


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 0F 08 88 F5 9F B0 D9 B2 87 52 DD 4A F6 BF 0D 5A 3D
17 34 A2


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: D6 D4 38 10 1E CE C6 62 90 73 47 7E 70 E4 7A 3
8 6D 05 EB 26
B0 1B 53 9B 1F A4 53 E7 BF FC 9F 04
SHA-1 Fingerprint: 4C 71 6A 5B 8A D8 E9 81 60 3F 10 4B 3E 15 28 DB
FE B7 ED 8D
MD5 Fingerprint: 77 34 E7 47 80 6C 3D 67 75 94 57 51 41 65 3E BF
```

192.168.15.112 (tcp/3389)

```
Subject Name:

Common Name: win81-qa-agent.localhost.local

Issuer Name:

Common Name: win81-qa-agent.localhost.local

Serial Number: 67 42 39 6A 4D 76 F2 80 41 77 B9 7B 0D DF 39 18

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption
```

```
Not Valid Before: May 15 21:36:18 2017 GMT
Not Valid After: Nov 14 21:36:18 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CC AC 68 75 12 CA 93 04 22 5C A1 50 04 A5 7A CD 65 5
F 1C
12 E0 26 43 13 B6 89 FE 4B CE 12 01 3D B0 D3 7D A7 9E C5 CA
20 5D 14 F2 4C D5 49 89 46 29 A1 62 7C 59 B9 52 6C 52 1B 1F
FF 03 65 79 E9 3D 36 0A 08 73 5A 24 EC 98 81 D8 B6 6C 49 A6
0E A6 38 0A D9 DE 90 4C 2E 8B C6 A9 04 2A BA E4 DD 33 76 57
D4 F9 1C E0 FB 49 D8 46 0F 67 40 2F E2 13 CC C9 38 E5 71 79
DD 55 7F 26 44 E3 30 E6 99 52 EF E2 1B D9 F7 D6 38 11 ED 6C
AE 13 14 5A D3 4D 3B 60 86 44 A0 98 5C DA A7 E0 0C 96 EB A2
11 E9 6F 18 59 2E D0 F2 6E C7 FF D9 79 DF 2B 7B B9 A5 5F 7A
77 6F 45 58 85 36 29 7C 1C 4F 4B 9B A8 11 BE 59 1B AB 6E A7
E3 F7 72 FA DF 0E 9D D1 3A AC B4 D5 C9 7F 0E D2 C9 43 6E 6F
91 A4 3D FC FA 33 7A 9F F6 11 1B 28 11 C6 6D 82 69 9D 6F 67
05 5D E8 AC 81 D6 17 42 29 96 06 CC B1 B9 CC B0 6D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 AB 6F 8C 27 C2 9E 7A 6C 9E 45 56 B0 0C 79 FA BF 90 23
95
C8 54 86 B9 9B 0D AC 72 BE 9C 56 39 10 94 98 FB 4A 36 CC DF
AE 19 75 6C B7 1C AB 4B 6B 44 1B C8 D4 4E 79 65 81 83 E5 7A
09 6C 44 A5 B0 5C E5 B4 7B 97 E7 13 41 6C 58 A4 C4 DA D2 1A
B0 62 2E 91 D7 3F B4 A7 AC AE D8 81 E7 3A AF B1 F3 00 8D 8E
DB 54 5F CD 3B 46 B1 C4 A0 4D 8B 57 11 FC BB 1F CB 8B CF CE
54 2A D9 CB 08 96 3B 4E 83 03 D2 F8 C4 3D 55 89 E1 63 D3 D7
B4 AA 09 11 C9 10 A8 4B CF AC F3 3F 8E C4 DA B7 3A 7C 31 99
65 E1 EE 0D 4F 75 4F 3E 90 3D 69 45 F7 7D 5F 57 0F 0A EE D6
FB DB D6 DA D3 79 11 4D CB 0F 9F 9E 5A 25 E0 29 DD 1A 52 40
F6 96 BF 9A 80 7C CD 17 95 50 53 C8 0B C0 24 48 42 6E BA CA
5E B2 A1 8F 26 ED 96 BB 8B D1 7C B2 50 48 79 66 09 97 51 C7
5B 60 1E E5 E1 72 CE 44 E4 5C EC 65 FC 20 8F 9F 9A

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment


Fingerprints :

SHA-256 Fingerprint: 76 3D 6E 65 26 28 34 7A 3D EB B7 76 95 9D 3B 5
2 2F 07 27 B2
76 5A E6 32 17 3B 40 C1 CF 5A 98 8D
SHA-1 Fingerprint: 77 1E C0 41 70 65 26 D3 26 5B 6D C0 ED 68 42 67
0A 90 BF 50
MD5 Fingerprint: B8 06 E1 99 62 C4 C6 55 2E BF B8 78 36 C1 15 22
```

192.168.15.113 (tcp/3389)

```
Subject Name:

Common Name: 2K8-QA-AGENT.localhost.local
```

```
Issuer Name:

Common Name: 2K8-QA-AGENT.localhost.local

Serial Number: 50 B1 57 88 60 C0 4F 97 44 86 79 73 D1 0B 29 05

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 15 21:07:47 2017 GMT
Not Valid After: Nov 14 21:07:47 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A8 77 D5 9D E2 FE FF 23 25 34 57 0A 6A 59 FD E2 80 D
8 BF
64 F1 8A 0A 20 E8 FE B6 1B B8 AF BB FA 2B BD E2 9E 90 1A B4
14 3B 07 B9 B5 83 6A 3A 32 69 67 D9 A8 5C 9F 01 D5 43 30 32
0A AE 9C BC E0 A7 0D 9A 03 BB C6 F4 8F DA E6 9F EF 6B B0 C0
11 3A BD 3C 90 31 B2 5B 3E 1B C2 CC 5F B6 A3 EF 22 D9 9B 4D
F9 D9 19 F2 44 89 BA DE C5 40 9E 0B 3D EB 3B 6D C9 64 24 12
05 22 4B 2A 80 D3 0E 76 8E F2 0C E3 BA 68 0D ED A4 B2 01 61
0E 07 E1 87 EB B5 85 9D B3 11 E5 E7 8B B4 22 6D 03 F6 BF EE
41 6D 47 D0 DF 16 DD FB 73 BC DD 4A DE 76 3B A5 27 82 3E EB
3A CE 99 BB 61 C3 41 9B 6A 0C B1 1B 8F 69 F2 DF 61 9B CD AB
75 0E 54 B1 CB 15 A4 E2 8D BB A5 9E A8 97 26 1A A7 79 CC E2
E7 76 DD CF 59 C5 69 06 8E 61 E6 C1 B5 C3 AF 60 96 55 8C E6
B9 B8 34 F7 A2 9A 15 96 EB F1 C4 86 A3 28 F7 04 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 49 0A C7 EB 55 52 2C 92 15 D2 05 5A D2 77 AE 99 F5 12
B7
5F F3 F6 7A 38 48 26 B3 DD AA 83 56 ED 12 E8 5B 4B FD 86 3B
2A 8D A1 3D 5B 35 22 1A 7C A2 50 50 A5 31 0E 40 43 79 7A 3D
15 50 38 69 E6 DA A0 61 E6 7B 95 89 25 22 62 C4 0B B7 7B 36
8A 32 43 65 D3 AD 44 3D 8F FA 74 1D 8F 34 DC 76 F7 13 7F B9
99 F6 00 BD 74 30 FC D0 ED 5E BA DD F5 59 53 5F E6 36 62 45
9B 7C C5 56 10 C1 8C 5F 9F E2 29 9F B2 17 EF 4B 66 1C 6B 41
CA 40 14 8D A2 D9 1B 61 EC BF AA 30 C2 8B 62 33 AE E7 DE 8A
4E 85 0E 5F 54 98 77 80 1A DA 13 9A 4A CE C9 BA 34 68 B5 12
88 CA 82 B8 BA 7A C6 96 10 AA 09 12 8F D1 CF 43 57 B4 2E 30
80 7E 7F BF 47 46 1D BA A9 8B 0F 2C 2C A9 AB BC 62 6E 2B AA
49 92 D0 DA 87 62 5F 33 74 C3 06 13 8B 21 83 C8 17 C6 BC 02
47 25 1B E3 DF C3 95 EE D7 D0 92 04 A2 66 79 73 2B

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment


Fingerprints :

SHA-256 Fingerprint: F3 D3 4A F8 24 E4 81 51 DE A3 FC FE 22 23 D6 1
5 77 FB A3 58
DD 06 D0 84 20 29 71 A5 0D EC C3 32
SHA-1 Fingerprint: B9 03 7B D3 50 BF 4D 1C CD DA 21 AF BE 94 43 3E
```

```
29 C0 EB 49
MD5 Fingerprint: E9 EE 32 3D 91 34 19 EE 24 F4 03 44 5A 93 08 59
```

10881 (3) - 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:

Publication date: 2002/03/06, Modification date: 2017/05/30

Hosts

192.168.15.43 (tcp/22)

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

- 1.99
- 2.0
```

192.168.15.72 (tcp/22)

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

- 1.99
- 2.0
```

192.168.15.85 (tcp/22)

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

- 1.99
- 2.0
```

11936 (3) - 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: 2017/02/21

Hosts

192.168.15.72 (tcp/0)

```
Remote operating system : Linux Kernel 3.10
Linux Kernel 3.13
Linux Kernel 4.2
Linux Kernel 4.8
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.10
Linux Kernel 3.13
Linux Kernel 4.2
Linux Kernel 4.8
```

192.168.15.112 (tcp/0)

```
Remote operating system : Microsoft Windows 8.1 Enterprise
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows 8.1 Enterprise
```

192.168.15.113 (tcp/0)

```
Remote operating system : Microsoft Windows Server 2008 R2 Enterpri
se Service Pack 1
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows Server 2008 R2 Enterpr
ise Service Pack 1
```

21643 (3) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2017/06/29

Hosts

192.168.15.43 (tcp/9090)

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
High Strength Ciphers (>= 112-bit key)
RSA-AES128-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA256
RSA-CAMELLIA256-SHA256 Kx=RSA Au=RSA Enc=Camellia-CBC(256) Mac=SHA2
56
RSA-CAMELLIA128-SHA256 Kx=RSA Au=RSA Enc=Camellia-CBC(128) Mac=SHA2
56
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
RSA-AES256-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA256
CAMELLIA128-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
CAMELLIA256-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
RSA-AES128-SHA256 Kx=RSA Au=RSA Enc=AES-GCM(128) Mac=SHA256
RSA-CAMELLIA-GCM-256 Kx=RSA Au=RSA Enc=Camellia-GCM(256) Mac=SHA384
n/a Kx=RSA Au=RSA Enc=AES-CCM(256) Mac=AEAD
RSA-AES256-SHA384 Kx=RSA Au=RSA Enc=AES-GCM(256) Mac=SHA384
RSA-CAMELLIA-GCM-128 Kx=RSA Au=RSA Enc=Camellia-GCM(128) Mac=SHA256
n/a Kx=RSA Au=RSA Enc=AES-CCM(128) Mac=AEAD


SSL Version : TLSv11
High Strength Ciphers (>= 112-bit key)
ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
CAMELLIA128-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
CAMELLIA256-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.112 (tcp/3389)

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
RSA-AES128-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
```

```
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
RSA-AES256-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA256
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1
ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1
ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.113 (tcp/3389)

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1
ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
```

```
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

24260 (3) - 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

Hosts

192.168.15.43 (tcp/9090)

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Security-Policy: default-src 'self' 'unsafe-inline'; connec
t-src 'self' ws: wss:
Transfer-Encoding: chunked
Cache-Control: no-cache, no-store
Connection: close
```

192.168.15.112 (tcp/10243)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 14 Jul 2017 17:32:04 GMT
Connection: close
Content-Length: 315
```

192.168.15.113 (tcp/47001)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
```

```
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 14 Jul 2017 17:29:18 GMT
Connection: close
Content-Length: 315
```

54615 (3) - 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

Hosts

192.168.15.72 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 59
```

192.168.15.112 (tcp/0)

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

192.168.15.113 (tcp/0)

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

56984 (3) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2017/06/15

Hosts

192.168.15.43 (tcp/9090)

```
This port supports TLSv1.1/TLSv1.2.
```

192.168.15.112 (tcp/3389)

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

192.168.15.113 (tcp/3389)

```
This port supports TLSv1.0.
```

66334 (3) - 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: 2017/07/11

Hosts

192.168.15.43 (tcp/0)

```
. You need to take the following action :
[ OpenSSH < 7.5 (99359) ]

+ Action to take : Upgrade to OpenSSH version 7.5 or later.
```

192.168.15.72 (tcp/0)

```
. You need to take the following action :
[ OpenSSH < 7.5 (99359) ]

+ Action to take : Upgrade to OpenSSH version 7.5 or later.

+Impact : Taking this action will resolve 7 different vulnerabiliti
es (CVEs).
```

192.168.15.85 (tcp/0)

```
. You need to take the following action :
[ OpenSSH < 7.5 (99359) ]
```

```
+ Action to take : Upgrade to OpenSSH version 7.5 or later.

+Impact : Taking this action will resolve 18 different vulnerabilit
ies (CVEs).
```

70657 (3) - SSH Algorithms and Languages Supported

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:

Publication date: 2013/10/28, Modification date: 2017/07/10

Hosts

192.168.15.43 (tcp/22)

```
Nessus negotiated the following encryption algorithm with the serve
r :

The server supports the following options for kex_algorithms :

curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for server_host_key_algor
ithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
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_algorithm
s_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithm
s_server_to_client :

none
zlib@openssh.com
```

192.168.15.72 (tcp/22)

```
Nessus negotiated the following encryption algorithm with the serve
r :

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_algor
ithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-dss
ssh-ed25519
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_algorithm
s_client_to_server :

none
zlib@openssh.com
```

```
The server supports the following options for compression_algorithm
s_server_to_client :

none
zlib@openssh.com
```

192.168.15.85 (tcp/22)

```
Nessus negotiated the following encryption algorithm with the serve
r :

The server supports the following options for kex_algorithms :

diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algor
ithms :

ssh-dss
ssh-rsa

The server supports the following options for encryption_algorithms
_client_to_server :

3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms
_server_to_client :

3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client
_to_server :

hmac-md5
hmac-md5-96
```

```
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com

The server supports the following options for mac_algorithms_server
_to_client :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com

The server supports the following options for compression_algorithm
s_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithm
s_server_to_client :

none
zlib@openssh.com
```

10107 (2) - 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

Hosts

192.168.15.112 (tcp/10243)

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

192.168.15.113 (tcp/47001)

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10150 (2) - 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: 2016/12/28

Hosts

192.168.15.112 (udp/137)

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

WIN81-QA-AGENT = Computer name
TEHGEEK = Workgroup / Domain name
WIN81-QA-AGENT = File Server Service
TEHGEEK = Browser Service Elections

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

00:15:5d:0f:c6:aa
```

192.168.15.113 (udp/137)

```
The following 3 NetBIOS names have been gathered :

2K8-QA-AGENT = File Server Service
2K8-QA-AGENT = Computer name
TEHGEEK = Workgroup / Domain name

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

00:15:5d:0f:c6:ab
```

10394 (2) - 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: 2017/01/19

Hosts

192.168.15.112 (tcp/445)

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

192.168.15.113 (tcp/445)

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

10785 (2) - 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:

Publication date: 2001/10/17, Modification date: 2017/02/21

Hosts

192.168.15.112 (tcp/445)

```
The remote Operating System is : Windows 8.1 Enterprise 9600
The remote native LAN manager is : Windows 8.1 Enterprise 6.3
The remote SMB Domain Name is : TEHGEEK
```

192.168.15.113 (tcp/445)

```
The remote Operating System is : Windows Server 2008 R2 Enterprise
7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Enterpris
e 6.1
The remote SMB Domain Name is : TEHGEEK
```

26917 (2) - 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

Hosts

192.168.15.112 (tcp/445)

```
Could not connect to the registry because:
Could not connect to IPC$
```

192.168.15.113 (tcp/445)

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

27576 (2) - Firewall Detection

Synopsis

The remote host is behind a firewall.

Description

Based on the responses obtained by the SYN or TCP port scanner, it was possible to determine that the remote host seems to be protected by a firewall.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/26, Modification date: 2012/02/22

Hosts

192.168.15.43 (tcp/0)

192.168.15.85 (tcp/0)

46180 (2) - 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:

Publication date: 2010/04/29, Modification date: 2017/04/27

Hosts

192.168.15.112 (tcp/0)

```
The following hostnames point to the remote host :
- win81-qa-agent
```

192.168.15.113 (tcp/0)

```
The following hostnames point to the remote host :
- 2k8-qa-agent
```

51891 (2) - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Hosts

192.168.15.112 (tcp/3389)

```
This port supports resuming TLSv1 sessions.
```

192.168.15.113 (tcp/3389)

```
This port supports resuming TLSv1 sessions.
```

53513 (2) - 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:

Publication date: 2011/04/21, Modification date: 2012/03/05

Hosts

192.168.15.112 (udp/5355)

```
According to LLMNR, the name of the remote host is 'win81-qa-agen
t'.
```

192.168.15.113 (udp/5355)

```
According to LLMNR, the name of the remote host is '2K8-QA-AGENT'.
```

64814 (2) - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/22, Modification date: 2017/06/15

Hosts

192.168.15.112 (tcp/3389)

```
Subject Name:

Common Name: win81-qa-agent.localhost.local

Issuer Name:
```

```
Common Name: win81-qa-agent.localhost.local

Serial Number: 67 42 39 6A 4D 76 F2 80 41 77 B9 7B 0D DF 39 18

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 15 21:36:18 2017 GMT
Not Valid After: Nov 14 21:36:18 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CC AC 68 75 12 CA 93 04 22 5C A1 50 04 A5 7A CD 65 5
F 1C
12 E0 26 43 13 B6 89 FE 4B CE 12 01 3D B0 D3 7D A7 9E C5 CA
20 5D 14 F2 4C D5 49 89 46 29 A1 62 7C 59 B9 52 6C 52 1B 1F
FF 03 65 79 E9 3D 36 0A 08 73 5A 24 EC 98 81 D8 B6 6C 49 A6
0E A6 38 0A D9 DE 90 4C 2E 8B C6 A9 04 2A BA E4 DD 33 76 57
D4 F9 1C E0 FB 49 D8 46 0F 67 40 2F E2 13 CC C9 38 E5 71 79
DD 55 7F 26 44 E3 30 E6 99 52 EF E2 1B D9 F7 D6 38 11 ED 6C
AE 13 14 5A D3 4D 3B 60 86 44 A0 98 5C DA A7 E0 0C 96 EB A2
11 E9 6F 18 59 2E D0 F2 6E C7 FF D9 79 DF 2B 7B B9 A5 5F 7A
77 6F 45 58 85 36 29 7C 1C 4F 4B 9B A8 11 BE 59 1B AB 6E A7
E3 F7 72 FA DF 0E 9D D1 3A AC B4 D5 C9 7F 0E D2 C9 43 6E 6F
91 A4 3D FC FA 33 7A 9F F6 11 1B 28 11 C6 6D 82 69 9D 6F 67
05 5D E8 AC 81 D6 17 42 29 96 06 CC B1 B9 CC B0 6D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 AB 6F 8C 27 C2 9E 7A 6C 9E 45 56 B0 0C 79 FA BF 90 23
95
C8 54 86 B9 9B 0D AC 72 BE 9C 56 39 10 94 98 FB 4A 36 CC DF
AE 19 75 6C B7 1C AB 4B 6B 44 1B C8 D4 4E 79 65 81 83 E5 7A
09 6C 44 A5 B0 5C E5 B4 7B 97 E7 13 41 6C 58 A4 C4 DA D2 1A
B0 62 2E 91 D7 3F B4 A7 AC AE D8 81 E7 3A AF B1 F3 00 8D 8E
DB 54 5F CD 3B 46 B1 C4 A0 4D 8B 57 11 FC BB 1F CB 8B CF CE
54 2A D9 CB 08 96 3B 4E 83 03 D2 F8 C4 3D 55 89 E1 63 D3 D7
B4 AA 09 11 C9 10 A8 4B CF AC F3 3F 8E C4 DA B7 3A 7C 31 99
65 E1 EE 0D 4F 75 4F 3E 90 3D 69 45 F7 7D 5F 57 0F 0A EE D6
FB DB D6 DA D3 79 11 4D CB 0F 9F 9E 5A 25 E0 29 DD 1A 52 40
F6 96 BF 9A 80 7C CD 17 95 50 53 C8 0B C0 24 48 42 6E BA CA
5E B2 A1 8F 26 ED 96 BB 8B D1 7C B2 50 48 79 66 09 97 51 C7
5B 60 1E E5 E1 72 CE 44 E4 5C EC 65 FC 20 8F 9F 9A

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

192.168.15.113 (tcp/3389)

```
Subject Name:

Common Name: 2K8-QA-AGENT.localhost.local

Issuer Name:
```

```
Common Name: 2K8-QA-AGENT.localhost.local

Serial Number: 50 B1 57 88 60 C0 4F 97 44 86 79 73 D1 0B 29 05

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 15 21:07:47 2017 GMT
Not Valid After: Nov 14 21:07:47 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A8 77 D5 9D E2 FE FF 23 25 34 57 0A 6A 59 FD E2 80 D
8 BF
64 F1 8A 0A 20 E8 FE B6 1B B8 AF BB FA 2B BD E2 9E 90 1A B4
14 3B 07 B9 B5 83 6A 3A 32 69 67 D9 A8 5C 9F 01 D5 43 30 32
0A AE 9C BC E0 A7 0D 9A 03 BB C6 F4 8F DA E6 9F EF 6B B0 C0
11 3A BD 3C 90 31 B2 5B 3E 1B C2 CC 5F B6 A3 EF 22 D9 9B 4D
F9 D9 19 F2 44 89 BA DE C5 40 9E 0B 3D EB 3B 6D C9 64 24 12
05 22 4B 2A 80 D3 0E 76 8E F2 0C E3 BA 68 0D ED A4 B2 01 61
0E 07 E1 87 EB B5 85 9D B3 11 E5 E7 8B B4 22 6D 03 F6 BF EE
41 6D 47 D0 DF 16 DD FB 73 BC DD 4A DE 76 3B A5 27 82 3E EB
3A CE 99 BB 61 C3 41 9B 6A 0C B1 1B 8F 69 F2 DF 61 9B CD AB
75 0E 54 B1 CB 15 A4 E2 8D BB A5 9E A8 97 26 1A A7 79 CC E2
E7 76 DD CF 59 C5 69 06 8E 61 E6 C1 B5 C3 AF 60 96 55 8C E6
B9 B8 34 F7 A2 9A 15 96 EB F1 C4 86 A3 28 F7 04 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 49 0A C7 EB 55 52 2C 92 15 D2 05 5A D2 77 AE 99 F5 12
B7
5F F3 F6 7A 38 48 26 B3 DD AA 83 56 ED 12 E8 5B 4B FD 86 3B
2A 8D A1 3D 5B 35 22 1A 7C A2 50 50 A5 31 0E 40 43 79 7A 3D
15 50 38 69 E6 DA A0 61 E6 7B 95 89 25 22 62 C4 0B B7 7B 36
8A 32 43 65 D3 AD 44 3D 8F FA 74 1D 8F 34 DC 76 F7 13 7F B9
99 F6 00 BD 74 30 FC D0 ED 5E BA DD F5 59 53 5F E6 36 62 45
9B 7C C5 56 10 C1 8C 5F 9F E2 29 9F B2 17 EF 4B 66 1C 6B 41
CA 40 14 8D A2 D9 1B 61 EC BF AA 30 C2 8B 62 33 AE E7 DE 8A
4E 85 0E 5F 54 98 77 80 1A DA 13 9A 4A CE C9 BA 34 68 B5 12
88 CA 82 B8 BA 7A C6 96 10 AA 09 12 8F D1 CF 43 57 B4 2E 30
80 7E 7F BF 47 46 1D BA A9 8B 0F 2C 2C A9 AB BC 62 6E 2B AA
49 92 D0 DA 87 62 5F 33 74 C3 06 13 8B 21 83 C8 17 C6 BC 02
47 25 1B E3 DF C3 95 EE D7 D0 92 04 A2 66 79 73 2B

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

70544 (2) - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Hosts

192.168.15.112 (tcp/3389)

```
Here is the list of SSL CBC ciphers supported by the remote server
:

High Strength Ciphers (>= 112-bit key)

TLSv1
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

192.168.15.113 (tcp/3389)

```
Here is the list of SSL CBC ciphers supported by the remote server
:

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
```

```
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

96982 (2) - 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:

Publication date: 2017/02/03, Modification date: 2017/02/16

Hosts

192.168.15.112 (tcp/445)

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

192.168.15.113 (tcp/445)

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

100871 (2) - 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:

Publication date: 2017/06/19, Modification date: 2017/06/19

Hosts

192.168.15.112 (tcp/445)

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

192.168.15.113 (tcp/445)

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

10386 (1) - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/04/28, Modification date: 2015/10/13

Hosts

192.168.15.43 (tcp/9090)

```
The following string will be used :
TYPE='password'
```

10940 (1) - 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

Hosts

192.168.15.112 (tcp/3389)

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:

Publication date: 2002/11/18, Modification date: 2017/06/08

Hosts

192.168.15.112 (tcp/2869)

```
A web server seems to be 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:

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

Hosts

192.168.15.113 (tcp/0)

```
It was not possible to connect to '\\2K8-QA-AGENT\ADMIN$' with the
supplied credentials.
```

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:

Publication date: 2009/02/19, Modification date: 2017/06/12

Hosts

192.168.15.112 (udp/1900)

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

http://192.168.15.112:2869/upnphost/udhisapi.dll?content=uuid:d099d
9f3-f884-4d6f-ac82-55c363b2296c

And advertises these unique service names :

uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c::urn:schemas-upnp-org:ser
vice:ContentDirectory:1
uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c::urn:schemas-upnp-org:dev
ice:MediaServer:1
uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c::urn:microsoft.com:servic
e:X_MS_MediaReceiverRegistrar:1
uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c::urn:schemas-upnp-org:ser
vice:ConnectionManager:1
uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c::upnp:rootdevice
```

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:

Publication date: 2009/02/19, Modification date: 2017/06/12

Hosts

192.168.15.112 (tcp/2869)

```
Here is a summary of http://192.168.15.112:2869/upnphost/udhisapi.d
ll?content=uuid:d099d9f3-f884-4d6f-ac82-55c363b2296c :

deviceType: urn:schemas-upnp-org:device:MediaServer:1
friendlyName: WIN81-QA-AGENT: admin:
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: S-1-5-21-2656180562-2369356312-3273087629-1001
ServiceID: urn:upnp-org:serviceId:ConnectionManager
serviceType: urn:schemas-upnp-org:service:ConnectionManager:1
```

```
controlURL: /upnphost/udhisapi.dll?control=uuid:d099d9f3-f884-4d6f-
ac82-55c363b2296c+urn:upnp-org:serviceId:ConnectionManager
eventSubURL: /upnphost/udhisapi.dll?event=uuid:d099d9f3-f884-4d6f-a
c82-55c363b2296c+urn:upnp-org:serviceId:ConnectionManager
SCPDURL: /upnphost/udhisapi.dll?content=uuid:e360b1ee-958f-40f0-ae6
2-a9935ad5be58
ServiceID: urn:upnp-org:serviceId:ContentDirectory
serviceType: urn:schemas-upnp-org:service:ContentDirectory:1
controlURL: /upnphost/udhisapi.dll?control=uuid:d099d9f3-f884-4d6f-
ac82-55c363b2296c+urn:upnp-org:serviceId:ContentDirectory
eventSubURL: /upnphost/udhisapi.dll?event=uuid:d099d9f3-f884-4d6f-a
c82-55c363b2296c+urn:upnp-org:serviceId:ContentDirectory
SCPDURL: /upnphost/udhisapi.dll?content=uuid:e29c43a7-1288-4410-952
b-08389deb3803
ServiceID: urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
serviceType: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:
1
controlURL: /upnphost/udhisapi.dll?control=uuid:d099d9f3-f884-4d6f-
ac82-55c363b2296c+urn:microsoft.com:serviceId:X_MS_MediaReceiverReg
istrar
eventSubURL: /upnphost/udhisapi.dll?event=uuid:d099d9f3-f884-4d6f-a
c82-55c363b2296c+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegi
strar
SCPDURL: /upnphost/udhisapi.dll?content=uuid:f1a59e02-59fc-4131-80f
a-6159c8302f56
```

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2017/06/12

Hosts

192.168.15.112 (tcp/3389)

```
Here is the list of SSL PFS ciphers supported by the remote server
:

High Strength Ciphers (>= 112-bit key)
```

```
TLSv1
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA256

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

84502 (1) - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information:

Publication date: 2015/07/02, Modification date: 2015/07/02

Hosts

192.168.15.43 (tcp/9090)

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

94761 (1) - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://technet.microsoft.com/en-us/library/cc778623

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2016/11/14, Modification date: 2016/11/14

Hosts

192.168.15.43 (tcp/9090)

```
The following root Certification Authority certificate was found :

|-Subject : O=5a4fa85e0277478f8c474a86c65f8daf/CN=fedora25.localhos
t.local
|-Issuer : O=5a4fa85e0277478f8c474a86c65f8daf/CN=fedora25.localhos
t.local
|-Valid From : Jan 23 22:14:10 2017 GMT
|-Valid To : Dec 30 22:14:10 2116 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

Remediations

[-] Collapse All

[+] Expand All

Suggested Remediations

Taking the following actions across 3 hosts would resolve 24% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
OpenSSH < 7.5 : Upgrade to OpenSSH version 7.5 or later.	14	2

This is a report from the Nessus Vulnerability Scanner .
Nessus is published by Tenable Network Security, Inc | 7021 Columbia Gateway Drive Suite 500, Columbia, MD 21046