CSS-Mars

Report generated by Nessus™ Sat, 31 Jul 2021 09:26:26 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.140.60

1	4	6	0	157
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Jul 31 09:08:37 2021
End time:	Sat Jul 31 09:26:26 2021

Host Information

Netbios Name:	CSS-MARS
IP:	192.168.140.60
MAC Address:	00:0C:29:49:9F:C1
OS:	Microsoft Windows

Vulnerabilities

147171 - Microsoft Exchange Server Authentication Bypass

Synopsis

The remote mail server is affected by an authentication bypass vulnerability.

Description

The Microsoft Exchange running on the remote host is affected by an authentication bypass vulnerability. An unauthenticated remote attacker can exploit this to execute arbitrary code.

See Also

http://www.nessus.org/u?14b26c05

http://www.nessus.org/u?fedb98e4

http://www.nessus.org/u?d9bf7dee

https://proxylogon.com/

http://www.nessus.org/u?4260a57a

Solution

Microsoft has released the following security updates to address this issue:

-KB5000871

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-26855
MSKB	5000871
XREF	MSFT:MS21-5000871

Exploitable With

Metasploit (true)

Plugin Information

Published: 2021/03/08, Modified: 2021/07/22

Plugin Output

tcp/443/www

```
Nessus was able to detect the issue by sending the following HTTP request to the remote host:

GET /owa/auth/x.js HTTP/1.1
Host: 192.168.140.60
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: X-AnonResource=true; X-AnonResource-Backend=localhost/ecp/default.flt?~3; X-
BEResource=localhost/owa/auth/logon.aspx?~3
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*


Nessus received the following response from the server:
```

```
HTTP/1.1 500 Internal Server Error
 Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
request-id: 43d73ebd-99e9-44eb-ab88-d29515f181ed
X-CalculatedBETarget: localhost
X-CalculatedBETarget: localhost
X-FEServer: CSS-MARS
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 31 Jul 2021 13:19:57 GMT
Connection: close
Content-Length: 97
 NegotiateSecurityContext failed with for host 'localhost' with status 'NoAuthenticatingAuthority'
```

35291 - 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?9bb87bf2

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

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
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=css-mars
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 31 10:04:52 2021 GMT
|-Valid To            : Jul 31 10:04:52 2026 GMT
```

35291 - 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?9bb87bf2

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

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/444/www

```

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=css-mars
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 31 10:04:52 2021 GMT
|-Valid To            : Jul 31 10:04:52 2026 GMT
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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/

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/443/www

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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/

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/444/www

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

    Name                          Code             KEX            Auth     Encryption             MAC
    ----------------------        ----------       ---            ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA            RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

51192 - 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

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

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

Solution

Purchase or generate a proper SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/443/www

```

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=css-mars
|-Issuer  : CN=css-mars
```

51192 - 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

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

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

Solution

Purchase or generate a proper SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/444/www

```
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=css-mars
|-Issuer  : CN=css-mars
```

57582 - 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 SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
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=css-mars
```

57582 - 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 SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/444/www

```
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=css-mars
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/443/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/444/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

10761 - COM+ Internet Services (CIS) Server Detection

Synopsis

A COM+ Internet Services (CIS) server is listening on this port.

Description

COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

See Also

http://www.nessus.org/u?d02f7e6e

https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp

Solution

If you do not use this service, disable it with DCOMCNFG.

Otherwise, limit access to this port.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/6001/ncacn_http

```

Server banner :

ncacn_http/1.0
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/07/22

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows

Following application CPE's matched on the remote system :

  cpe:/a:microsoft:exchange_server:
  cpe:/a:microsoft:exchange_server:15.1.2176.2
  cpe:/a:microsoft:iis:10.0
  cpe:/a:microsoft:outlook_web_access:15.1.2176.2
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/135/epmap

```

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 : WMsgKRpc087FE0

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 : WMsgKRpc087FE0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE60047759B57CD3322A3720C1E4C0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-acc5bbc1a574adfa3b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000001
UUID : f3f09ffd-fbcf-4291-944d-70ad6e0e73bb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cb3fdee7ba1d1f31cf

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d2716e94-25cb-4820-bc15-537866578562, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEB8C89674C151836BC3D1F527678F

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d2716e94-25cb-4820-bc15-537866578562, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRP [...]
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/445/cifs

```

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 : \\CSS-MARS

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 : \\CSS-MARS

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 : \\CSS-MARS

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 : \\CSS-MARS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\CSS-MARS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\CSS-MARS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\CSS-MARS

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 : \\CSS-MARS

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

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/2103/dce-rpc

```

The following DCERPC services are available on TCP port 2103 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.140.60
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/2105/dce-rpc

```

The following DCERPC services are available on TCP port 2105 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.140.60
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/2107/dce-rpc

```

The following DCERPC services are available on TCP port 2107 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.140.60
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6400/dce-rpc

```
The following DCERPC services are available on TCP port 6400 :

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 : 6400
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6401/dce-rpc

```

The following DCERPC services are available on TCP port 6401 :

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 : 6401
IP : 192.168.140.60

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 : 6401
IP : 192.168.140.60

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 : 6401
IP : 192.168.140.60

Object UUID : b5ccd5ef-4238-440b-bba0-999f828f1cfe
```

```
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6401
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6401
IP : 192.168.140.60

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 : 6401
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6402/dce-rpc

```
The following DCERPC services are available on TCP port 6402 :

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 : 6402
IP : 192.168.140.60

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 : 6402
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 6402
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
```

```
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 6402
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 6402
IP : 192.168.140.60

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 : 6402
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6403/dce-rpc

```

The following DCERPC services are available on TCP port 6403 :

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 : 6403
IP : 192.168.140.60

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 : 6403
IP : 192.168.140.60

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 : 6403
IP : 192.168.140.60

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 : 6403
IP : 192.168.140.60

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 : 6403
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6413/dce-rpc

```
The following DCERPC services are available on TCP port 6413 :

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 : 6413
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6424/dce-rpc

```

The following DCERPC services are available on TCP port 6424 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 6424
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 6424
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 6424
IP : 192.168.140.60
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 6424
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6425/dce-rpc

```

The following DCERPC services are available on TCP port 6425 :

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 : 6425
IP : 192.168.140.60

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 : 6425
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 6425
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
```

```
Type : Remote RPC service
TCP Port : 6425
IP : 192.168.140.60

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 : 6425
IP : 192.168.140.60

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 : 6425
IP : 192.168.140.60

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 : 6425
IP : 192.168.140.60

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 : 6425
IP : 192.168.140.60

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description :  [...]
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6478/dce-rpc

```

The following DCERPC services are available on TCP port 6478 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4d88f820-8c32-4453-9e30-7297e2fcf025, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6478
IP : 192.168.140.60

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 684MSExchangeThrottling
Type : Remote RPC service
TCP Port : 6478
IP : 192.168.140.60

Object UUID : 082dca90-cc8d-46e8-be8e-4d851fc938df
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 684MSExchangeThrottling
Type : Remote RPC service
TCP Port : 6478
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6479/dce-rpc

```
The following DCERPC services are available on TCP port 6479 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f1f21151-7185-4170-ac8d-9bb077c29bd3, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6479
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6480/dce-rpc

```
The following DCERPC services are available on TCP port 6480 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 832Microsoft.Exchange.Search.Service
Type : Remote RPC service
TCP Port : 6480
IP : 192.168.140.60

Object UUID : 60356ff0-12b8-4d88-9626-92c8d62fb9a2
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 832Microsoft.Exchange.Search.Service
Type : Remote RPC service
TCP Port : 6480
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ecca92d9-07d1-4136-87f7-2ac4109337ee, version 7.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6480
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6483/dce-rpc

```

The following DCERPC services are available on TCP port 6483 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3336Microsoft.Exchange.ServiceHost
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 574624b3-6365-471a-8122-7862ee2a90fc
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3336Microsoft.Exchange.ServiceHost
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d9318e75-8a8b-4abb-88e7-aceb01f09e60, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20434699-5e7e-47d6-95f6-698c4a0ec2f0, version 1.0
Description : Unknown RPC service
```

```
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 37c6221b-cc4b-47ae-8366-7449f2fe9a06, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fd9e884-86a5-4b2f-bc7c-2adaa75d0469, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b396a3ff-9203-4c75-a367-244cf29b419f, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d014c423-0d54-40a3-90dc-56c7a6071e6f, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 245a2854-fcdf-4215-adf4-0b4c364e79fb, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6483
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6493/dce-rpc

```
The following DCERPC services are available on TCP port 6493 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3472MSExchangeDelivery
Type : Remote RPC service
TCP Port : 6493
IP : 192.168.140.60

Object UUID : 695194e6-3dac-4ac0-9463-54f1ff3f1bfb
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3472MSExchangeDelivery
Type : Remote RPC service
TCP Port : 6493
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6509/dce-rpc

```
The following DCERPC services are available on TCP port 6509 :

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 : 6509
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6513/dce-rpc

```

The following DCERPC services are available on TCP port 6513 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3992Microsoft.Exchange.RpcClientAccess.Service
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60

Object UUID : f812b574-43c3-469b-9989-69d4803a60e7
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3992Microsoft.Exchange.RpcClientAccess.Service
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5261574a-4572-206e-b268-6b199213b4e4, version 0.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a4f1db00-ca47-1067-b31f-00dd010662da, version 0.0
Description : Exchange Server STORE EMSMDB Interface
```

```
Windows process : store.exe
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ba3fa067-8d56-4b56-ba1f-9cbae8db3478, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1544f5e0-613c-11d1-93df-00c04fd7bd09, version 1.0
Description : MS Exchange Directory RFR Interface
Windows process : unknown
Annotation : Microsoft Exchange RFR Interface
Type : Remote RPC service
TCP Port : 6513
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6514/dce-rpc

```

The following DCERPC services are available on TCP port 6514 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 52d3f3f5-248c-4d74-a01f-a06e41d5cd59, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6514
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6523/dce-rpc

```
The following DCERPC services are available on TCP port 6523 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 89742ace-a9ed-11cf-9c0c-08002be7ae86, version 2.0
Description : Exchange Server STORE ADMIN Interface
Windows process : store.exe
Annotation : Exchange Server STORE Admin20 Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 99e64010-b032-11d0-97a4-00c04fd6551d, version 4.0
Description : Exchange Server STORE ADMIN Interface
Windows process : store.exe
Annotation : Exchange Server STORE Admin40 Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : da107c01-2b50-44d7-9d5f-bfd4fd8e95ed, version 5.0
Description : Unknown RPC service
Annotation : Exchange Server STORE Admin50 Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 938fe036-ede6-4f6c-966e-a3d7300279c8, version 0.0
Description : Unknown RPC service
Annotation : Exchange Server STORE EmsmdbPool Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b48e5eb-b4cd-4b6d-ae73-656e0a777bda, version 0.0
Description : Unknown RPC service
Annotation : Exchange Server STORE EmsmdbPoolNotify Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : df831451-edad-415d-905f-9d3793f92db3, version 0.0
Description : Unknown RPC service
Annotation : Exchange Server STORE EmsmdbMT Proxy Interface
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 31e68719-d4fc-401a-8788-bc56169a336b, version 0.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6523
IP : 192.168.140.60

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255 [...]
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6582/dce-rpc

```
The following DCERPC services are available on TCP port 6582 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 424MSExchangeCompliance
Type : Remote RPC service
TCP Port : 6582
IP : 192.168.140.60

Object UUID : 07bf777d-b7ed-43bb-babe-ea2e41d6d96c
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 424MSExchangeCompliance
Type : Remote RPC service
TCP Port : 6582
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6583/dce-rpc

```
The following DCERPC services are available on TCP port 6583 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 972umservice
Type : Remote RPC service
TCP Port : 6583
IP : 192.168.140.60

Object UUID : 276ca922-56c7-4842-a294-23b105b2e236
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 972umservice
Type : Remote RPC service
TCP Port : 6583
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6584/dce-rpc

```

The following DCERPC services are available on TCP port 6584 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3344MSExchangeFrontendTransport
Type : Remote RPC service
TCP Port : 6584
IP : 192.168.140.60

Object UUID : 3402854b-47cd-41ae-8193-41d84360b65d
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3344MSExchangeFrontendTransport
Type : Remote RPC service
TCP Port : 6584
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6585/dce-rpc

```
The following DCERPC services are available on TCP port 6585 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 568MSExchangeSubmission
Type : Remote RPC service
TCP Port : 6585
IP : 192.168.140.60

Object UUID : c6b19014-cdf8-4f4f-8d63-95622834bc2c
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 568MSExchangeSubmission
Type : Remote RPC service
TCP Port : 6585
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6586/dce-rpc

```

The following DCERPC services are available on TCP port 6586 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3368MSExchangeMailboxAssistants
Type : Remote RPC service
TCP Port : 6586
IP : 192.168.140.60

Object UUID : e3b2da53-a925-4bac-9a6d-5908b2512c6f
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3368MSExchangeMailboxAssistants
Type : Remote RPC service
TCP Port : 6586
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a020372-bb0a-4031-a5a7-7c6896522c00, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6586
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c0d124-a18e-49d4-adf1-d8c6ba868ea6, version 1.0
Description : Unknown RPC service
```

```
Type : Remote RPC service
TCP Port : 6586
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6587/dce-rpc

```
The following DCERPC services are available on TCP port 6587 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4048MSExchangeMailboxReplication
Type : Remote RPC service
TCP Port : 6587
IP : 192.168.140.60

Object UUID : 19bd5b2c-d1af-4f85-882a-0dac7a9a05c3
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4048MSExchangeMailboxReplication
Type : Remote RPC service
TCP Port : 6587
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6611/dce-rpc

```
The following DCERPC services are available on TCP port 6611 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4076Microsoft.Exchange.UM.CallRouter
Type : Remote RPC service
TCP Port : 6611
IP : 192.168.140.60

Object UUID : f2798e0a-57b3-45d6-a50f-5a07339c415e
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4076Microsoft.Exchange.UM.CallRouter
Type : Remote RPC service
TCP Port : 6611
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6617/dce-rpc

```

The following DCERPC services are available on TCP port 6617 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 520msexchangerepl
Type : Remote RPC service
TCP Port : 6617
IP : 192.168.140.60

Object UUID : ad10ae74-dbe5-41ad-9afc-71fb26ab9252
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 520msexchangerepl
Type : Remote RPC service
TCP Port : 6617
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 37fc1b02-da36-4b27-a745-bf2f58a98ff6, version 3.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6617
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f224209f-9076-40f7-98ad-5416dbfa178e, version 3.0
Description : Unknown RPC service
```

```
  Type : Remote RPC service
  TCP Port : 6617
  IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6655/dce-rpc

```
The following DCERPC services are available on TCP port 6655 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 1244MSExchangeTransport
Type : Remote RPC service
TCP Port : 6655
IP : 192.168.140.60

Object UUID : 21898ba3-f1e4-4574-a015-ad248ef5a410
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 1244MSExchangeTransport
Type : Remote RPC service
TCP Port : 6655
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6665/dce-rpc

```

The following DCERPC services are available on TCP port 6665 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7376EdgeTransport
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60

Object UUID : 7a0bacc1-4606-4563-8716-cc07e9784f6c
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7376EdgeTransport
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8384fc47-956a-4d1e-ab2a-1205014f96ec, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bd5790c9-d855-42b0-990f-3dfed8c184b3, version 1.0
Description : Unknown RPC service
```

```
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 640aa52e-d472-443a-952c-4d3fe97f480c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 41f5fae1-e0ac-414c-a721-0d287466cb23, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6665
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6677/dce-rpc

```

The following DCERPC services are available on TCP port 6677 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7596MSExchangeServicesAppPool
Type : Remote RPC service
TCP Port : 6677
IP : 192.168.140.60

Object UUID : 9fc4ce62-5c6a-40ba-bea7-e94ef15e4f3c
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7596MSExchangeServicesAppPool
Type : Remote RPC service
TCP Port : 6677
IP : 192.168.140.60

Object UUID : c61bdb8f-265a-4d85-a7d9-1ab81e4bb9c0
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7596MSExchangeServicesAppPool
Type : Remote RPC service
TCP Port : 6677
IP : 192.168.140.60

```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6683/dce-rpc

```

The following DCERPC services are available on TCP port 6683 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4604noderunner
Type : Remote RPC service
TCP Port : 6683
IP : 192.168.140.60

Object UUID : ee6bd71e-36b2-4d39-9c26-5d4d14d22dcc
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 4604noderunner
Type : Remote RPC service
TCP Port : 6683
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6685/dce-rpc

```

The following DCERPC services are available on TCP port 6685 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1febdc2a-1734-4e06-8998-ed919c26ad43, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e62eb024-ee96-4d89-b24a-746cf02a3e98, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8879d5aa-30a7-4eb2-9023-bec055dbe648, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d3444dd6-ee15-4564-83fc-0b16b8f5e8d4, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
```

```
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6f08d61c-fd57-42b0-bb11-f30aedaca66e, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2d0ca50-457a-4d87-ab1e-45f3a324993f, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ea0c3893-d1fd-4fb3-82d0-8e9a86486dc5, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 75f47e04-c7c9-411e-a9eb-080b174b03a9, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 6685
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6764/dce-rpc

```

The following DCERPC services are available on TCP port 6764 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7316MSExchangeOWAAppPool
Type : Remote RPC service
TCP Port : 6764
IP : 192.168.140.60

Object UUID : 4649f9a4-75cd-4fed-b9cb-cc8a17ac69b0
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7316MSExchangeOWAAppPool
Type : Remote RPC service
TCP Port : 6764
IP : 192.168.140.60

Object UUID : 9e841fa9-1e59-4bfd-8948-02b2ef51cb75
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 7316MSExchangeOWAAppPool
Type : Remote RPC service
TCP Port : 6764
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/6784/dce-rpc

```
The following DCERPC services are available on TCP port 6784 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 9288MSExchangeECPAppPool
Type : Remote RPC service
TCP Port : 6784
IP : 192.168.140.60

Object UUID : 057d10d9-6dc1-422e-b915-bf5b51eb94bd
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 9288MSExchangeECPAppPool
Type : Remote RPC service
TCP Port : 6784
IP : 192.168.140.60

Object UUID : 3face3f5-c710-4c0a-af04-c0017a3c6ead
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 9288MSExchangeECPAppPool
Type : Remote RPC service
TCP Port : 6784
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7023/dce-rpc

```
The following DCERPC services are available on TCP port 7023 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a4d59fe-42ac-4c6e-b554-b12c6af35956, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 7023
IP : 192.168.140.60

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 6052MSExchangeHMHost
Type : Remote RPC service
TCP Port : 7023
IP : 192.168.140.60

Object UUID : 2c12e195-4e11-49fc-9688-5e6d31ee612b
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 6052MSExchangeHMHost
Type : Remote RPC service
TCP Port : 7023
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7061/dce-rpc

```

The following DCERPC services are available on TCP port 7061 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10736MSExchangeOWACalendarAppPool
Type : Remote RPC service
TCP Port : 7061
IP : 192.168.140.60

Object UUID : 5891ddef-f2b7-4d12-bfe2-6dac7adbc9ec
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10736MSExchangeOWACalendarAppPool
Type : Remote RPC service
TCP Port : 7061
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7072/dce-rpc

```

The following DCERPC services are available on TCP port 7072 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11044MSExchangeSyncAppPool
Type : Remote RPC service
TCP Port : 7072
IP : 192.168.140.60

Object UUID : bfb654f6-c8b0-4915-abc7-7786f0ac4f60
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11044MSExchangeSyncAppPool
Type : Remote RPC service
TCP Port : 7072
IP : 192.168.140.60

Object UUID : d64ffa1b-50e3-47bc-a421-64d403923a92
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11044MSExchangeSyncAppPool
Type : Remote RPC service
TCP Port : 7072
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7094/dce-rpc

```
The following DCERPC services are available on TCP port 7094 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10320MSExchangePowerShellFrontEndAppPool
Type : Remote RPC service
TCP Port : 7094
IP : 192.168.140.60

Object UUID : b07c71b3-c34f-48ef-8341-38769a84f579
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10320MSExchangePowerShellFrontEndAppPool
Type : Remote RPC service
TCP Port : 7094
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7119/dce-rpc

```
The following DCERPC services are available on TCP port 7119 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3016MSExchangeOABAppPool
Type : Remote RPC service
TCP Port : 7119
IP : 192.168.140.60

Object UUID : b9a193e6-5d67-402c-b778-938378f067f9
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 3016MSExchangeOABAppPool
Type : Remote RPC service
TCP Port : 7119
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7132/dce-rpc

```

The following DCERPC services are available on TCP port 7132 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10388MSExchangeMapiFrontEndAppPool
Type : Remote RPC service
TCP Port : 7132
IP : 192.168.140.60

Object UUID : 9be5e3ec-9984-407f-87b3-e34e1ebbd183
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10388MSExchangeMapiFrontEndAppPool
Type : Remote RPC service
TCP Port : 7132
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7146/dce-rpc

```
The following DCERPC services are available on TCP port 7146 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11628MSExchangeRpcProxyAppPool
Type : Remote RPC service
TCP Port : 7146
IP : 192.168.140.60

Object UUID : 10e05b1f-eb30-447b-831c-e967061b5df1
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11628MSExchangeRpcProxyAppPool
Type : Remote RPC service
TCP Port : 7146
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7169/dce-rpc

```

The following DCERPC services are available on TCP port 7169 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11956MSExchangePowerShellAppPool
Type : Remote RPC service
TCP Port : 7169
IP : 192.168.140.60

Object UUID : 9df4c0ff-2420-4a68-a03c-7d9381f12052
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11956MSExchangePowerShellAppPool
Type : Remote RPC service
TCP Port : 7169
IP : 192.168.140.60

Object UUID : 7a23ff37-8b84-4143-a314-41c66f071b29
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 11956MSExchangePowerShellAppPool
Type : Remote RPC service
TCP Port : 7169
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7189/dce-rpc

```
The following DCERPC services are available on TCP port 7189 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2360MSExchangeAutodiscoverAppPool
Type : Remote RPC service
TCP Port : 7189
IP : 192.168.140.60

Object UUID : a09a65b1-59ce-41c2-a56c-107f5bbb55b8
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2360MSExchangeAutodiscoverAppPool
Type : Remote RPC service
TCP Port : 7189
IP : 192.168.140.60

Object UUID : c4b09285-3ed4-47ae-80e0-55a295a34142
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2360MSExchangeAutodiscoverAppPool
Type : Remote RPC service
TCP Port : 7189
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7203/dce-rpc

```

The following DCERPC services are available on TCP port 7203 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2328MSExchangeRpcProxyFrontEndAppPool
Type : Remote RPC service
TCP Port : 7203
IP : 192.168.140.60

Object UUID : 448fb63f-597c-41e8-aad5-3992cb474616
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2328MSExchangeRpcProxyFrontEndAppPool
Type : Remote RPC service
TCP Port : 7203
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7237/dce-rpc

```
The following DCERPC services are available on TCP port 7237 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10444MSExchangeMapiMailboxAppPool
Type : Remote RPC service
TCP Port : 7237
IP : 192.168.140.60

Object UUID : beecd214-139f-45dc-9ade-d926ef910fe7
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 10444MSExchangeMapiMailboxAppPool
Type : Remote RPC service
TCP Port : 7237
IP : 192.168.140.60
```

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/7324/dce-rpc

```
The following DCERPC services are available on TCP port 7324 :

Object UUID : 37518031-bba5-48de-98dc-8bccff43b608
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2196MSExchangeRestAppPool
Type : Remote RPC service
TCP Port : 7324
IP : 192.168.140.60

Object UUID : 3f6e358c-c5d7-4452-9c61-6a14cd25fba8
UUID : 5df3c257-334b-4e96-9efb-a0619255be09, version 1.0
Description : Unknown RPC service
Annotation : 2196MSExchangeRestAppPool
Type : Remote RPC service
TCP Port : 7324
IP : 192.168.140.60
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 80
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```

The following card manufacturers were identified :

00:0C:29:49:9F:C1 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:49:9F:C1
```

84502 - 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). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. 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

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.
```

84502 - 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). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. 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

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/444/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/444/www

```
Based on the response to an OPTIONS request :
  - HTTP methods  GET  HEAD  POST  TRACE OPTIONS are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/81/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/444/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Microsoft-IIS/10.0
  Date: Sat, 31 Jul 2021 13:18:40 GMT
  Content-Length: 0

Response Body :

```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/81/www

```

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Sat, 31 Jul 2021 13:18:40 GMT
  Content-Length: 1233

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
```

```
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-
serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you
 supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/443/www

```

Response Code : HTTP/1.1 302 Moved Temporarily

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Cache-Control: no-cache
  Pragma: no-cache
  Location: https://192.168.140.60/owa/
  Server: Microsoft-IIS/10.0
  X-FEServer: CSS-MARS
  X-RequestId: 07a2bc51-c86c-470f-aede-9717a8fbb96f
  Date: Sat, 31 Jul 2021 13:18:40 GMT
  Connection: close
  Content-Length: 0

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/444/www

```

Response Code : HTTP/1.1 500 Internal Server Error

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

  Cache-Control: private
  Content-Type: text/html; charset=utf-8
  Server: Microsoft-IIS/10.0
  X-AspNet-Version: 4.0.30319
  X-Powered-By: ASP.NET
  Date: Sat, 31 Jul 2021 13:18:40 GMT
  Content-Length: 3490

Response Body :

<!DOCTYPE html>
<html>
    <head>
        <title>Runtime Error</title>
        <meta name="viewport" content="width=device-width" />
        <style>
         body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
         p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
         b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
         H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
         H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
         pre {font-family:"Consolas","Lucida Console",Monospace;font-
size:11pt;margin:0;padding:0.5em;line-height:14pt}
         .marker {font-weight: bold; color: black;text-decoration: none;}
         .version {color: gray;}
         .error {margin-bottom: 10px;}
         .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:pointer; }
         @media screen and (max-width: 639px) {
          pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
         }
         @media screen and (max-width: 479px) {
          pre { width: 280px; }
         }
        </style>
    </head>
    <body bgcolor="white">
            <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>
            <h2> <i>Runtime Error</i> </h2></span>
            <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">
            <b> Description: </b>An application error occurred on the server. The current custom
 error settings for this application prevent the details o [...]
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/03, Modified: 2021/07/22

Plugin Output

tcp/25/smtp

```
  Path    :
  Version : unknown
  Source  : SMTP
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/03, Modified: 2021/07/22

Plugin Output

tcp/444/www

```
Path    : /owa/auth/logon.aspx
Version : 15.1.2176.2
Source  : HTTP/HTTPS
major   : 15
minor   : 1
patch   : 2176
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/03, Modified: 2021/07/22

Plugin Output

tcp/465/smtp

```

  Path    :
  Version : unknown
  Source  : SMTP
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/03, Modified: 2021/07/22

Plugin Output

tcp/587/smtp

```

  Path    :
  Version : unknown
  Source  : SMTP
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/03, Modified: 2021/07/22

Plugin Output

tcp/2525/smtp

```

  Path    :
  Version : unknown
  Source  : SMTP
```

14255 - Microsoft Outlook Web Access (OWA) Version Detection

Synopsis

It is possible to extract the version of Microsoft Exchange Server installed on the remote host.

Description

Microsoft Exchange Server with Outlook Web Access (OWA) embeds the Exchange version number inside the default HTML web page. By requesting the default HTML page, Nessus was able to extract the Microsoft Exchange server version.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/11, Modified: 2021/01/19

Plugin Output

tcp/444/www

```
  URL     : https://192.168.140.60:444/owa/auth/logon.aspx
  Version : 15.1.2176.2
  CU      : 6
```

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

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

 CSS-MARS          = Computer name
 MEGACORP          = Workgroup / Domain name
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2020/01/22

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server 2016 Standard Evaluation 14393
The remote native LAN manager is : Windows Server 2016 Standard Evaluation 6.3
The remote SMB Domain Name is : MEGACORP
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

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

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```

The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/25/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/81/www

```
Port 81/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/135/epmap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/139/smb

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/444/www

```
Port 444/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/445/cifs

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/465/smtp

```
Port 465/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/475/smtp

```
Port 475/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/476/smtp

```
Port 476/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/477/smtp

```
Port 477/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/587/smtp

```
Port 587/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/593/http-rpc-epmap

```
Port 593/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/808

```
Port 808/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/1801

```
Port 1801/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/2103/dce-rpc

```
Port 2103/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/2105/dce-rpc

```
Port 2105/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/2107/dce-rpc

```
Port 2107/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/2525/smtp

```
Port 2525/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/3875

```
Port 3875/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/5060/sip

```
Port 5060/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/5065

```
Port 5065/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6001/ncacn_http

```
Port 6001/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6400/dce-rpc

```
Port 6400/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6509/dce-rpc

```
Port 6509/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6514/dce-rpc

```
Port 6514/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6582/dce-rpc

```
Port 6582/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

tcp/6665/dce-rpc

```
Port 6665/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/06/28

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.15.0
Nessus build : 20271
Plugin feed version : 202107310212
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : CSS-Mars
Scan policy used : Basic Network Scan
Scanner IP : 192.168.140.128
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 78.680 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
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 : 2021/7/31 9:09 EDT
Scan duration : 989 sec
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows
Confidence level : 80
Method : SMTP

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

SMTP:220 css-mars.MEGACORP.COM Microsoft ESMTP MAIL Service ready at Sat, 31 Jul 2021 15:11:02
 +0200\n220 css-mars.MEGACORP.COM MICROSOFT ESMTP MAIL SERVICE READY AT Sat, 31 Jul 2021 15:13:18
 +0200
HTTP:Server: Microsoft-IIS/10.0

SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181500_7_p=443
SSLcert:!:i/CN:css-marss/CN:css-mars
a98312992aee2b4c314cc73182b4420bec09e63a
i/CN:css-marss/CN:css-mars
a98312992aee2b4c314cc73182b4420bec09e63a
```

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

21745 - OS Security Patch Assessment Failed

Synopsis

Errors prevented OS Security Patch Assessment.

Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

Risk Factor

None

References

XREF	IAVB:0001-B-0501

Plugin Information

Published: 2006/06/23, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following service errors were logged :

  - Plugin      : smb_login.nasl
    Plugin ID   : 10394
    Plugin Name : Microsoft Windows SMB Log In Possible
    Protocol    : SMB
    Message     :
It was not possible to log into the remote host via smb (invalid credentials).
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2021/07/13

Plugin Output

tcp/0

```


. You need to take the following action :

[ Microsoft Exchange Server Authentication Bypass (147171) ]

+ Action to take : Microsoft has released the following security updates to address this issue:
  -KB5000871


```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM Microsoft ESMTP MAIL Service ready at Sat, 31 Jul 2021 15:11:02 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM Microsoft ESMTP MAIL Service ready at Sat, 31 Jul 2021 15:14:01 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/475/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM MICROSOFT ESMTP MAIL SERVICE READY AT Sat, 31 Jul 2021 15:13:18 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/476/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM MICROSOFT ESMTP MAIL SERVICE READY AT Sat, 31 Jul 2021 15:13:23 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/477/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM MICROSOFT ESMTP MAIL SERVICE READY AT Sat, 31 Jul 2021 15:14:23 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/587/smtp

```

Remote SMTP server banner :

220 css-mars.MEGACORP.COM Microsoft ESMTP MAIL Service ready at Sat, 31 Jul 2021 15:11:02 +0200
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/2525/smtp

```
Remote SMTP server banner :

220 css-mars.MEGACORP.COM Microsoft ESMTP MAIL Service ready at Sat, 31 Jul 2021 15:13:27 +0200
```

56984 - 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

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - 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

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/444/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

10863 - 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

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: css-mars

Issuer Name:

Common Name: css-mars

Serial Number: 52 27 59 52 2A A4 2C BD 41 CD 37 C2 B4 7A A6 11

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 31 10:04:52 2021 GMT
Not Valid After: Jul 31 10:04:52 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 97 62 62 DC F3 63 50 F5 57 69 6A A9 F4 06 0A 33 19 B1 A8
            62 53 CF 7E 7D 3E AB C7 53 64 50 19 07 BA 83 3A 45 01 E0 5E
            DA 08 B8 94 27 91 2F F4 20 CA 46 72 56 96 48 FC 84 4A D3 5D
            57 69 97 0B 61 D1 CF 73 F4 C2 89 EF 6E 87 6F 3E DE 3E 9F AF
            34 72 46 E7 A1 B3 78 8A 21 07 09 2E CA 57 C6 4B 5C D0 A2 FE
            49 C8 16 75 DD D9 24 C3 E9 0A 75 6C FA EF 78 95 37 22 E9 B6
            B0 FF 53 44 7D 0C 07 54 4B 7D 6E E3 9D 23 ED 87 F4 FF 66 70
            97 5A 43 1F D5 E5 AD CF 40 B6 58 E0 99 AC 27 70 AC 2C 4B AB
            7D 9B 4E EB 21 66 9D 8D DC 65 03 0B 21 43 AA C6 12 63 21 BF
            38 D7 9E 89 85 24 3E 02 F1 F3 C1 31 BB 1A F6 42 11 DD AC C5
            CA 90 D8 F4 49 7A 43 F0 A8 EE EA 71 9F A9 6E 18 0F 6E 1E E4
            C1 96 1E AB D9 28 F1 2D F9 E2 42 BD A9 E2 2E F4 D6 8C C8 9A
            02 BD E6 91 D3 D9 E6 82 01 BF E2 0D F9 55 80 9C C9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7C 96 0A 69 61 99 54 C6 52 F5 E1 00 A7 E4 56 34 8C 96 FC
           40 33 87 3C 5B 8F E5 2F 19 51 70 03 83 3F DE D2 CF C1 7D 62
           A1 2F 8A 80 17 86 E7 F8 66 B3 81 D7 65 D3 18 5F 76 EB 78 FB
           8D 27 A4 5C 00 32 7E E2 70 49 E7 9E C6 5A FD 9E 44 90 2E DB
           A7 8B E7 3A D4 F7 7D 71 BF 6D D2 EB 31 37 C4 1A E6 4E DB B8
           90 03 AB 71 E5 A6 E0 DD 5E D9 10 57 C2 10 A8 21 27 97 B1 60
           5C 86 E0 9C B4 A1 3B 69 31 B1 A6 9B 40 1D E8 1C F7 87 B9 42
           4E 41 9F 84 67 96 23 45 1A A7 95 1A 87 3B 5D 1C C1 3D 17 86
           D4 5A 42 BD A7 AC 6B 07 CE 39 19 A5 D3 DA 97 93 5D 6F C8 D8
           4E 85 CB 15 1E 6B 1B 40 34 75 F6 E [...]
```

10863 - 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

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/444/www

```
Subject Name:

Common Name: css-mars

Issuer Name:

Common Name: css-mars

Serial Number: 52 27 59 52 2A A4 2C BD 41 CD 37 C2 B4 7A A6 11

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 31 10:04:52 2021 GMT
Not Valid After: Jul 31 10:04:52 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 97 62 62 DC F3 63 50 F5 57 69 6A A9 F4 06 0A 33 19 B1 A8
            62 53 CF 7E 7D 3E AB C7 53 64 50 19 07 BA 83 3A 45 01 E0 5E
            DA 08 B8 94 27 91 2F F4 20 CA 46 72 56 96 48 FC 84 4A D3 5D
            57 69 97 0B 61 D1 CF 73 F4 C2 89 EF 6E 87 6F 3E DE 3E 9F AF
            34 72 46 E7 A1 B3 78 8A 21 07 09 2E CA 57 C6 4B 5C D0 A2 FE
            49 C8 16 75 DD D9 24 C3 E9 0A 75 6C FA EF 78 95 37 22 E9 B6
            B0 FF 53 44 7D 0C 07 54 4B 7D 6E E3 9D 23 ED 87 F4 FF 66 70
            97 5A 43 1F D5 E5 AD CF 40 B6 58 E0 99 AC 27 70 AC 2C 4B AB
            7D 9B 4E EB 21 66 9D 8D DC 65 03 0B 21 43 AA C6 12 63 21 BF
            38 D7 9E 89 85 24 3E 02 F1 F3 C1 31 BB 1A F6 42 11 DD AC C5
            CA 90 D8 F4 49 7A 43 F0 A8 EE EA 71 9F A9 6E 18 0F 6E 1E E4
            C1 96 1E AB D9 28 F1 2D F9 E2 42 BD A9 E2 2E F4 D6 8C C8 9A
            02 BD E6 91 D3 D9 E6 82 01 BF E2 0D F9 55 80 9C C9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7C 96 0A 69 61 99 54 C6 52 F5 E1 00 A7 E4 56 34 8C 96 FC
           40 33 87 3C 5B 8F E5 2F 19 51 70 03 83 3F DE D2 CF C1 7D 62
           A1 2F 8A 80 17 86 E7 F8 66 B3 81 D7 65 D3 18 5F 76 EB 78 FB
           8D 27 A4 5C 00 32 7E E2 70 49 E7 9E C6 5A FD 9E 44 90 2E DB
           A7 8B E7 3A D4 F7 7D 71 BF 6D D2 EB 31 37 C4 1A E6 4E DB B8
           90 03 AB 71 E5 A6 E0 DD 5E D9 10 57 C2 10 A8 21 27 97 B1 60
           5C 86 E0 9C B4 A1 3B 69 31 B1 A6 9B 40 1D E8 1C F7 87 B9 42
           4E 41 9F 84 67 96 23 45 1A A7 95 1A 87 3B 5D 1C C1 3D 17 86
           D4 5A 42 BD A7 AC 6B 07 CE 39 19 A5 D3 DA 97 93 5D 6F C8 D8
           4E 85 CB 15 1E 6B 1B 40 34 75 F6 E [...]
```

70544 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/www

```

Here is the list of SSL CBC ciphers supported by the remote server :

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

70544 - 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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/444/www

```

Here is the list of SSL CBC ciphers supported by the remote server :

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

21643 - 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

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/443/www

```

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)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
```

```
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168) [...]
```

21643 - 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

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/444/www

```
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)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
```

```
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168) [...]
```

57041 - 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

https://www.openssl.org/docs/manmaster/man1/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

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

```

Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

```
    Kex={key exchange}
    Auth={authentication}
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

57041 - 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

https://www.openssl.org/docs/manmaster/man1/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

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/444/www

```

Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

```
    Kex={key exchange}
    Auth={authentication}
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

51891 - 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

Published: 2011/02/07, Modified: 2020/08/17

Plugin Output

tcp/443/www

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

51891 - 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

Published: 2011/02/07, Modified: 2020/08/17

Plugin Output

tcp/444/www

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

96982 - 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/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

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

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

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

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF	IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/25/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/81/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/443/www

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

tcp/443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/444/www

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

tcp/444/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/465/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/475/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/476/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/477/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/587/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/593/http-rpc-epmap

```
An http-rpc-epmap is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/2525/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/6001/ncacn_http

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

21642 - Session Initiation Protocol Detection

Synopsis

The remote system is a SIP signaling device.

Description

The remote system is running software that speaks the Session Initiation Protocol (SIP).

SIP is a messaging protocol to initiate communication sessions between systems. It is a protocol used mostly in IP Telephony networks / systems to setup, control, and teardown sessions between two or more systems.

See Also

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

Solution

If possible, filter incoming connections to the port so that it is used only by trusted sources.

Risk Factor

None

Plugin Information

Published: 2003/12/29, Modified: 2019/11/22

Plugin Output

tcp/5060/sip

```
Nessus found an unidentified SIP service.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2021/02/03

Plugin Output

tcp/443/www

```

  http/1.1
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2021/02/03

Plugin Output

tcp/444/www

```
http/1.1
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/444/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/444/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

104410 - Target Credential Status by Authentication Protocol - Failure for Provided Credentials

Synopsis

Nessus was unable to log into the detected authentication protocol, using the provided credentials, in order to perform credentialed checks.

Description

Nessus failed to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials.

There may have been a failure in protocol negotiation or communication that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may have been invalid. A protocol failure may indicate a compatibility issue with the protocol configuration. A protocol failure due to an environmental issue such as resource or congestion issues may also prevent valid credentials from being identified. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

Address the reported problem(s) so that credentialed checks can be executed.

Risk Factor

None

References

XREF	IAVB:0001-B-0503

Plugin Information

Published: 2017/11/06, Modified: 2020/10/19

Plugin Output

tcp/445/cifs

```
Nessus was unable to log into the following host for which
credentials have been provided :

  Protocol        : SMB
  Port            : 445
  Failure details :

  - User : megacorp\administrator

    - Plugin      : smb_login.nasl
      Plugin ID   : 10394
      Plugin Name : Microsoft Windows SMB Log In Possible
      Message     :
Failed to authenticate using the supplied credentials.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.140.128 to 192.168.140.60 :
192.168.140.128
192.168.140.60

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

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

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/07/19

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

33139 - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man

https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985

```

Here is some information about the WS-Management Server :

  Product Vendor  : Microsoft Corporation
  Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

10386 - 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

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/443/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    https://192.168.140.60/rw_z4NIaqm7J.html
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

tcp/445/cifs

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

 CSS-MARS          = Computer name
 MEGACORP          = Workgroup / Domain name
```