M3W12D4 – RemediationMeta

Analisi delle vulnerabilità e azioni di rimedio

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti. Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - ScansioneInizio.pdf
2. Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - ScansioneFine.pdf
   Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

---

Il risultato del report finale, una volta rimandata la scansione con gli stessi parametri è la seguente:

Ultimo scan

Report generated by Tenable Nessus™ Mon, 10 Feb 2025 12:41:35 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.60.101

5	6	28	8	116
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.60.101
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Synopsis

The remote SSL certificate uses a weak key.

Exploitable With

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/25/smtp

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Synopsis

The remote SSL certificate uses a weak key.

Exploitable With

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/5432/postgresql

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

CVSS v2.0 Base Score

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/25/smtp

```
- SSLv2 is enabled and the server supports at least one cipher.



    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       -----         ----     ---------------------  ---
    EXP-RC2-CBC-MD5                                RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                                    RSA(512)      RSA      RC4(40)                MD5
       export

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                                   RSA           RSA      3DES-CBC(168)          MD5

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                                        RSA           RSA      RC4(128)               MD5

The fields above are :



  {Tenable ciphername}

  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}

  Encrypt={symmetric encryption method}
  MAC={message authentication code}

  {export flag}



    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       -----         ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA                        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                            DH            RSA      DES-CBC(56)            SHA
 [...]
```

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

CVSS v2.0 Base Score

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

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

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS v2.0 Base Score

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/5432/postgresql

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3



     Name                              Code             KEX           Auth     Encryption             MAC
     ----------------------            ----------       ---           ----     ---------------------  ---
     EDH-RSA-DES-CBC3-SHA                               DH            RSA      3DES-CBC(168)
 SHA1
                                                       RSA           RSA      3DES-CBC(168)
    DES-CBC3-SHA

   High Strength Ciphers (>= 112-bit key)

     Name                              Code             KEX           Auth     Encryption             MAC
     ----------------------            ----------       ---           ----     ---------------------  ---
     DHE-RSA-AES128-SHA                                 DH            RSA      AES-CBC(128)
  SHA1
     DHE-RSA-AES256-SHA                                 DH            RSA      AES-CBC(256)
  SHA1
     AES128-SHA                                         RSA           RSA      AES-CBC(128)
  SHA1
     AES256-SHA                                         RSA           RSA      AES-CBC(256)
  SHA1
     RC4-SHA                                            RSA           RSA      RC4(128)
  SHA1

The fields above are :



  {Tenable ciphername}

  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```