METASPLOITABLE

CAJA NEGRA

CRITICAS No INTER4ESANTES:

# La vulnerabilidades criticas detectadas en modo ejecutivo, ninguna afecta a la maquina ya que, éstas se refieren a puertas traseras y ejecución de código malicioso en versiones PHP < 5.4.43, así como al servicio Ftp anónimo y al programa IRCdemoin y phpMyAdmin.

# La Maquina de estudio presenta instalada la versión 5-4.5 PHP, por lo que no se vería afectada por esta vulnerabilidad, únicamente encontrando una dependencia etiquetada como low por exitir relación con el servicio “Get request” que puede ser usado para ejecutar esta vulnerabilidad.

# HIGH NO INTERESANTES

# 1.- Drupal Database Abstraction API SQLi

# No tiene instalada la maquina la aplicación Drupal que es la afectada por ella

# 2.-

HIGH 9.3\* - 67260 PHP 5.4.x < 5.4.17 Buffer Overflow

HIGH 7.5\* 6.7 71427 PHP 5.4.x < 5.4.23 OpenSSL openssl\_x509\_parse() Memory Corruption

HIGH 7.2\* 6.7 73862 PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation

HIGH 7.5\* 5.9 76281 PHP 5.4.x < 5.4.30 Multiple Vulnerabilities

HIGH 7.5\* 6.7 78545 PHP 5.4.x < 5.4.34 Multiple Vulnerabilities

# HIGH 7.5\* 6.6 80330 PHP 5.4.x < 5.4.36 'process\_nested\_data' RCE

# )HIGH 7.3 5.9 66585 PHP 5.4.x < 5.4.13 Information Disclosure

# HIGH 7.3 5.9 69401 PHP 5.4.x < 5.4.19 Multiple Vulnerabilities

# HIGH 7.3 6.7 81080 PHP 5.4.x < 5.4.37 Multiple Vulnerabilities

# HIGH 7.3 3.6 85298 PHP 5.4.x < 5.4.44 Multiple Vulnerabilities

# HIGH 7.3 6.7 85885 PHP 5.4.x < 5.4.45 Multiple Vulnerabilities

# Todas estas no les afecta a la maquina ya que como hemos dicho tiene la versión 5.4.5 de pHP

# 3.- SSL Medium Strength Cipher Suites Supported (SWEET32):

# Esta vuelnabilidad afecta a cualquier cifrado que utilice longitudes de claves de al menos 64 bits y menos de 112 bits, o bien que utilice la suite de cifrado 3DES.

# La máquina analizada uno de los cifrados que soporta es el “3des-cbc”, pero analizados las medidas e los cifrados que utiliza sus servicios no tiene ninguno entre 64 a 112bits , además tiene puerto 443 cerrado.

# 4.- Generic SQL Injection (blind).- es uan vulnerabilidad que afecta a servidosres que tiene instalado algún servicio SQL. Un aves examinada el dispositivo, no se encuentra dicha apliacion , por lo que no le afecta .

# HIGH INTERESANTES:

# 1.- PHP 7.3.24 Vulnerabilidades múltiples

# EL equipo tiene instalado la versión PHP 5.4.5, puedo provocar múltiples vulnerabilidades remotamente, siendo la solución actualizar a la versión PHP 7.3.24 o posterior. Existe un control de cambio con fecha de 4 de junio de 2024 donde aconsejan que la opción “Habilitar cgi escaneado” este en “true”.

# Según lo consulatado en la web “php.net”, la versión que menos vulnerabilidades tiene es la 7.4.33, existiendo versiones 8.0, las cuales presentan muchas vulnerabilidades, no existiendo exploits públicos conocidos.

# Tiene una valor CVSS de un 7.5 pero no tiene VPR alguno, por lo que entiendo que no es urgente.

# MEDIUM NO INTERESANTES

# 1 y 2 - TLS Version 1.0 Protocol Detection y TLS Version 1.1 Deprecated Protocol.- Ambas vulnerabilidades prersentan un CVSS de severidad de un 6.5, no teniendo putunción VPR referente a la urgencia del cambio. Estas se refieren al cifrado remoto con versiones antiguas TLS, como la TLS 1.0, aocnsejando actualziar a las versiones 1.2 y 1.3 y deshabilitar la 1.0, ya qye este ultimo tiene fallas de seguridad de diseño criptografico, puediendo actores maliciosos llevar a cabo ataques MITM o descifrado de las comunicaciones .

# Comprobada lña maquina objeto de estudio no usa el protocolo SSL 1.0 por lo que no l afectarían estas vulnerabilidades

# 

# 3.- SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795).- Esta vulnerabiliodad esta clasificada con una severidad de 5.9 pero con una urgencia de intervención de 6.1, la cual se refiere al ataque por truncamiento de prefijo de MITM, conocida como “Terrapin”, pudiendo permitir un ataque “Man in the Middle” eludiendo la integridad y seguridad de la conexión si usan openSSH en versiones anteriores a la versión 9.6, y que soporten ChaCha20-Poly1305 o CBC con Encrypt-then-MAC, siendo vulnerable a otros servicios entre los que se encuentran: como otros servicios como Apache MINA sshd a 2.11.0, TinySSH a 20230101, FileZilla antes de 3.66.4, KiTTY a 0.76.1.13, Netgate pfSense Plus a 23.09.1, Netgate pfSense CE a 2.7.2, Netgate pfSense Plus a 23.09.1, Netgate pfSense CE a 2.7.2.

# 

# 

# Se comprueba los protocolos y metodos de encriptación que utiliza la maquina objetvo de estudio, comprobando que usan los protocolos SSL v3, TLS v1.2 y como métodos AES, RSA, SHA1,SHA256, MD5, entre otros

# 

# Tampoco utiliza cifrado ChaCha-20 y, como hemos dicho anteriormente, los CBC usados son SSL v3 con MAC= SHA1, por lo que no seria vulnerable .

# 4.- Browsable Web Directories.- Esta vulnerabilidad presenta una severidad de 5.3, sin aportar información sobre la urgencia para su resolución, afectando a directorios de un servidor web remoto navegables que puedan filtrar información confidencial, siendo dependiente de otra vulnerabilidad “Apache Multiviews Atrarbitrar Listado de Directory”, pudiendo ser afectado por un ataque de divulgación de información, recomendando tener instalado una versión Apche superior a la 1.2.22. El equipo analizado tiene una versión más nueva, por lo que no sería vulnerable.

# Tampoco tiene instalado la versión Apache vulnerable, teniendo el Apache 2 de fecha de junio de 2024. Tampoco presenta el resto de versiones nombradas.

# 

# 5.- PHP 5.4.x < 5.4.12 Information Disclosure.- La version que tiene instalada la maquina objetivo es una versión superior a la que expresa esta vulnerabilidad, por lo que no es vulnarable.

# 

# 6.- SMB Signing not required.- Esta vulnerabilidad afecta al protocolo SMB, que es usado por la aplicación Samba en Linux, para conectar dispositivos en una red como impresoras, etc. Se comprueba la el archivo smb.conf de samba, no apareciendo ninguna anotación al SMB. Se ejecuta el comnado testparm -s, para chequear el fichero smb.conf, tampoco mostrando nada sobre eset protocolo:

# 

# Por último se comprueba el estado del SMB, no encontrando conexiones SMB por lo que se deduce que no utiliza SMB , no estando afectado por esta vulnerabilidad y existen exploits públicos para ello.

# 

# 7,8,9,10,11,12.- PHP 5.4.x < 5.4.16 Multiple Vulnerabilities, PHP 5.4.x < 5.4.24 Multiple Vulnerabilities, PHP 5.4.x < 5.4.26 Multiple Vulnerabilities, PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS, PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities, PHP 5.4.x < 5.4.32 Multiple Vulnerabilities, PHP 5.4.x < 5.4.35 'donote' DoS

# Todas estas vulnerabilidades afectan a servidores con la versión PHP inferiores a la 5.4.35, teniendo el dispositivo analizado la versión PHP 5.4.5.

# MEDIUM INTERESANTE

# 1.- IP Forwarding Enabled.- Esta vulnerabilidad tiene un valor alto de medio de severidad y de urgencia de actuación(6.5 y 4.0), consistiendo en que actores maliciosos pueden acceder al sistema si tienen activado el servidor remoto, aconsejando en este último caso, deshabilitar el reenviado de IP, salvo que el host sea un router, ya que podrían explotar esta debilidad para enrutar paquetes a través del huésped, y potencialmnente eludiendo cortafuegos/Routers/filtrado Mac.

# En caso de Linux para desactivar:” echo 0 - /proc/sys/net/ipv4/ip-forward” , en Windows” HKEY,LOCAL-MACHINE-System-CurrentControlSet-Services-Tcpip-Parameters” y en MAC OS X “sysctl -w net.inet.ip.forwarding=0”.

# 2 y 3 .- SSL Certificate Cannot Be Trusted.- Esta vulnerabilidad presenta un CVSS de carácter medio, sin tener puntuación VPR, afectando al certificado X.509 del servidor, encontrando mucha similitud con otra vulnerabilidad encontrada en el escaneo: SSL Self-Signed Certificate, la cual tb se aprovecha de la vulnerabilidad de los certificados X.509.

# Un certificado X.509 es un estándar de formato para los certificados de clave pública. Estos certificados se utilizan en diversas aplicaciones de seguridad, como SSL/TLS para sitios web seguros.

# Esta debilidad podría facilitar la realización de ataques por actores maliciosos tipo “MITM”, habida cuenta que usando certificados vulnerables, se puede romper la cadena de confianza de las siguientes formas:

# El encabezado del certificado enviada al servidor podria ser un certificado no reconocido y autofirmado, o pueden faltar certificados intermedios que conecten con el encabezado de un certificado de autoridad publica.

# Cuando se escanea el certificado antes de una de las fechas de inicio en el campo “noantes” del certificado o después de las fechas del campo “no después” del mismo, pudiendo contener certificados no valido.

# La cadena de certificados puede contener una firma que no coincida con la información del certificado, o no pudo ser verificado.

# Para impedir esto se recomienda generar certificados SSL adecuados, así como asegurarse de que el reloj del sistema esté correctamente sincronizado con un servidor de tiempo confiable (NTP) y monitorear las fechas de expiración de los certificados y renovación antes de que expiren, encontrándose una renovación corregida con fecha de octubre de 2023:

# 4.- PHP < 7.3.28 Email Header Injection.- Esta vulnerabilidad tiene una severidad de 5.3, no teniendo puntuación sobre la urgencia en su resolución, la cual, ejecuta en el servidor web remoto una inyección de encabezado de correo electrónico, si tiene una versión anterior de PHP a la 7.3.28.

# Esta se produce debido a un fallo en el manejo de la secuencias de CR-LF en los campos de encabezado, aprovechando esta situación actores maliciosos para insertar caracteres en la línea de encabezados del correo electrónico, obteniendo un control total del contenido de dichos encabezados, siendo su solución actualizar a la versión indicada anteriormente o superior de PHP y cambiando la opción “habilitar CGI escaneado” a la opción “true”( modificación del 4 de junio de 2004).

# 5.- CGI Genérico XSS (prueba exhaustiva).- Esta vulnerabilidad presenta una severidad de 4.3, sin puntuación de urgencia en resolución, donde servidores web pueden ser propensos a ataques XSS no persistentes, el cual consiste en aprovechar que los scripts CGI de la web no logran desinfectar adecuadamente las cadenas de solicitud de scripts malicioso, pudiendo ser capaces actores maliciosos de hacer que el código HTML y el script se ejecuten de forma conjunta en el navegador de un usuario dentro del contexto de seguridad del sitio web afectado

# Este script hace además de espejo del sitio web remoto y extraer la lista de CGI que son utilizados por el huésped remoto.

# La solución que proponen es reestablecer el acceso a la aplicación vulnerable o usar parches de actualización.

# 6.- Web Application Potentially Vulnerable to Clickjacking. - Esta vulnerabilidad para Linux y Windows, presenta una severidad de 4.3 de puntuación, sin tener valor alguno en cuanto a la urgencia de su resolución. Ejecutándose en un servidor web remoto que no configura la cabecera de respuesta adecuadamente (X-frame-Options o Frame-ancestors), exponiendo el sitio web a un ataque de “clickjacking”, en el que actores maliciosos pueden engañar a los usuarios de la web, para que al hacer click en una zona de la web que han vulnerado, esta realice acciones fraudulentas o maliciosas sobre el mismo, el cual no es capaz de percibir el cambio en la zona de la web.

# Los métodos X-Frame-Options y Content-Security-Policy no son los únicos que pueden evitar este tipo de ataques, existiendo actualmente métodos más confiables a través de la automatización. No obstante, pueden producirse falsos positivos si se despliegan junto a otras estrategias.

# La solución a esta vulnerabilidad es devolver el encabezado HTTP con alguno de estos métodos (con la directiva ‘frame-ancestors’) con la respuesta de la página, evitando que el contenido sea renderizado por otra web cuando utilice el marco o las etiquetas HTML iframe

# LOW

# 1.- SSH Weak MAC Algorithms Enabled. - Esta vulnerabilidad presenta un puntuaciñón de severidad de 2.6 puntos y sin valor en la urgencia de intervención, afectando al servidor SSH configurado para usar Cipher Block Chaining (CBC), pudiendo permitir al atacante recuperar el mensaje de texto plano del cifrado.

# La solución a este problema es configurar las opciones del servidor SSH que desactive el cifrado CBC y habilite el cifrado de modo CTR o GCM:

# CTR (Counter Mode) es un modo cifrado en bloque que convierte éste, en un cifrado de flujo, es decir, en lugar de cifrar bloques de datos directamente, genera un flujo de claves que se combina con los datos.

# GCM (Galois/Counter Mode) es un modo de cifrado de bloque que proporciona tanto confidencialidad como integridad de los datos, combinando el modo CTR para el cifrado con un código de autenticación de mensajes (MAC).

# El dispositivo Metasploitable analizado no es vulnerable, ya que no usa certificados CBC en SSH

# 

# WEB

# <https://www.tenable.com/plugins/nessus/142591>

# <https://www.tenable.com/plugins/nessus/50686>

# <https://www.tenable.com/plugins/nessus/51192>

# <https://www.tenable.com/plugins/nessus/57582>

# <https://www.tenable.com/plugins/nessus/104743>

# <https://www.tenable.com/plugins/nessus/157288>

# <https://cwe.mitre.org/data/definitions/327>

# <https://www.tenable.com/plugins/nessus/187315>

# <https://terrapin-attack.com/index.html#question-answer>

# <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2023-48795>

# <https://www.tenable.com/plugins/nessus/40984/changelog>

# <https://www.tenable.com/plugins/nessus/152853>

# <https://www.tenable.com/plugins/nessus/57608>

# <https://www.tenable.com/plugins/nessus/85582>

# <https://www.tenable.com/plugins/nessus/47831/dependencies>

# <http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>