Open-CHARGEN (Character Generator Protocol)

1. INTRODUCCIÓN

El Protocolo generador de caracteres (CHARGEN) es un servicio de la Familia de Protocolos de Internet definido en la RFC 864 y diseñado para fines de prueba, depuración y medición.

Un host puede conectarse a un servidor que soporta el CharGen en el puerto número 19 con TCP o UDP. Al abrir una conexión TCP, el servidor comienza a enviar caracteres arbitrarios al host de conexión hasta que el host cierre la conexión. En UDP el servidor envía un datagrama UDP que contiene un número aleatorio de caracteres (entre 0 y 512), cada vez que recibe un datagrama desde el host.

Ciertos protocolos UDP tienen respuestas a ciertos comandos que son mucho más grandes que la petición inicial. Donde un solo paquete puede generar decenas o cientos de veces el ancho de banda en su respuesta (un ataque de amplificación).

Algunos protocolos UDP, y sus factores de amplificación de ancho de banda (BAF), que han sido identificados como posibles vectores de ataque se enumeran a continuación:

Protocolo	Bandwidth Amplification Factor
DNS	28 a 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	**358.8**
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-017A

2. RIESGO

UDP, es un protocolo no orientado a conexión que no valida las direcciones IP de origen, a menos que el protocolo de capa de aplicación utilice mecanismos de inicio de sesión. Cuando el paquete UDP tiene la dirección IP de origen falsificada (victima), el servidor responde a la víctima, creando un ataque de Denegación reflejada de servicio (RDoS).

Un ataque DRDOS (*Distributed Reflective Denial of Service*) es una forma de ataque DDoS (*Distributed Denial of Service*) que se basa en el uso de servidores UDP de acceso público y en BAF, para congestionar a un sistema víctima con tráfico UDP. El atacante suplanta la IP de la víctima y envía muchas solicitudes al servidor, la respuesta de CHARGEN va a ser mayor que la solicitud, quien las recibe va a ser la víctima y no el atacante, la victima recibe inundaciones con tráfico no deseado, ataque DDoS.

3. DETECCIÓN

El reporte de "Open CharGen" se basa en peticiones UDP al puerto 19 de servidores con direcciones IPv4, si CharGen está habilitado como respuesta se espera ver gran cantidad de texto aleatorio.

La comprobación se realiza usando el siguiente comando en Linux:

nc -u [IP] 19

Se escribe algunos caracteres y se los borra, si CharGen está activado aparecerá texto aleatorio en la pantalla.

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Nombre de la vulnerabilidad reportada
Dirección IP	Dirección IP del host
Puerto	Puerto desde donde se obtiene la respuesta
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
status_EcuCERT	Online: vulnerabilidad reportada por el *Feed* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por el *Feed*, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del host
protocol	Protocolo por el que ingresó la respuesta (UDP)
port	Puerto desde donde se obtiene la respuesta Chargen
hostname	DNS reverso del host
tag	Siempre será chargen
size	Tamaño de la respuesta recibida (en bytes)
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado/Provincia/Región donde se encuentra el host
city	Ciudad donde se encuentra el host

4. ACCIONES RECOMENDADAS

Desactivar el servicio o bloquear el puerto de no utilizarse.

Verificación de la IP de origen

Rechazar cualquier tráfico UDP con direcciones falsificadas (spoofed). El IETF publicó como un ISP puede filtrar el tráfico de red para rechazar los paquetes con direcciones de origen no accesibles a través de la ruta del paquete, que hacen que el dispositivo de enrutamiento evalúe si es posible llegar a la dirección IP de origen del paquete a través de la interfaz que transmitió el paquete, si no es posible es probable que el paquete tenga una dirección IP de origen falso.

Catalogación de tráfico (Traffic Shaping)

Limitar respuestas a las peticiones UDP, requiere de pruebas para descubrir el límite óptimo que no interfiera con el tráfico legítimo. La IETF describe algunos métodos en las RFCs 2475 y 3260 para controlar el tráfico, actualmente muchos dispositivos de red ofrecen estas funciones en su software.

5. REFERENCIAS

- https://chargenscan.shadowserver.org/
- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Chargen https://www.us-cert.gov/ncas/alerts/TA14-017A
- http://www.iss.net/security_center/reference/vuln/Chargen_Denial_of_Service.htm
- http://tools.ietf.org/html/bcp38
  (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)
- http://tools.ietf.org/html/bcp84
  (Ingress Filtering for Multihomed Networks)