Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069	Fecha: 20-03-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El nuevo ataque 'Loop DoS' afecta a cientos de miles de sistemas		
Tipo de Ataque	Denegación de servicio DoS	Abreviatura	DoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. ANTECEDENTES:

Se ha descubierto que un novedoso vector de ataque de denegación de servicio (DoS) se dirige a protocolos de capa de aplicación basados en el Protocolo de datagramas de usuario (UDP), poniendo en riesgo a cientos de miles de hosts.

2. DETALLES:

Conocidos como ataques Loop DoS, estos métodos consisten en emparejar "servidores de dichos protocolos de forma que se desencadene una comunicación perpetua entre ellos", según los investigadores del CISPA Helmholtz-Center for Information Security.

Debido a su diseño inherente, UDP es un protocolo sin conexión que no verifica las direcciones IP de origen, por lo que es propenso a la suplantación de IP.

Por lo tanto, cuando los atacantes falsifican varios paquetes UDP para incluir la dirección IP de la víctima, el servidor de destino responde a la víctima (a diferencia del actor de la amenaza), creando un ataque de denegación de servicio (DoS) reflejado.

El último estudio encontró que ciertas implementaciones del protocolo UDP, como DNS, NTP, TFTP, Active Users, Daytime, Echo, Chargen, QOTD y Time, pueden usarse como armas para crear un bucle de ataque que se perpetúa a sí mismo.

"Empareja dos servicios de red de tal manera que siguen respondiendo indefinidamente a los mensajes del otro", dijeron los investigadores. "Al hacerlo, crean grandes volúmenes de tráfico que resultan en una denegación de servicio para los sistemas o redes involucradas. Una vez que se inyecta un disparador y el bucle se pone en movimiento, ni siquiera los atacantes pueden detener el ataque".

En pocas palabras, dados dos servidores de aplicaciones que ejecutan una versión vulnerable del protocolo, un actor de amenazas puede iniciar la comunicación con el primer servidor falsificando la dirección del segundo servidor, lo que hace que el primer servidor responda a la víctima (es decir, el segundo servidor) con un mensaje de error.

La víctima, a su vez, también mostrará un comportamiento similar, enviando otro mensaje de error al primer servidor, agotando efectivamente los recursos de cada uno y haciendo que cualquiera de los servicios no responda.

"Si un error como entrada crea un error como salida, y un segundo sistema se comporta igual, estos dos sistemas seguirán enviando mensajes de error de un lado a otro indefinidamente", explicaron Yepeng Pan y Christian Rossow.

3. RECOMENDACIONES:

- Mantener medidas para filtrar el tráfico falsificado.
- Configurar filtros en el router para controlar el acceso y el tráfico de paquetes.
- Instalar y mantener actualizados los últimos parches de seguridad de su software.
- Utilizar soluciones de seguridad integrales con protección en tiempo real y que te permita detectar y bloquear malware.

Fuente de Información:	• hxxps://thehackernews.com/2024/03/new-loop-dos-attack-impacts-hundreds-of.html • hxxps://hackarizona.org/es/cientos-de-miles-de-sistemas-afectados-por-un-nuevo-ataque-loop-dos/