BOLETÍN DE ALERTA

Boletín Nro.: 2020-32

Fecha de publicación: 05/11/2020

Tema: Técnica NAT Slipstreaming, vulnerabilidad que elude protecciones de NAT/Firewall y permite el acceso a servicios TCP/UDP.

Descripción:

Un investigador de seguridad ha revelado recientemente los detalles técnicos de una técnica llamada **NAT Slipstreaming** para eludir los controles de seguridad del **firewall** o **NAT (Network Address Translation)** y acceder remotamente a cualquier servicio TCP/UDP.

NAT es el proceso en el que un dispositivo de red, como puede ser un firewall o routers, reasigna un espacio de direcciones IP a otro modificando la información de la dirección de red en el encabezado IP de los paquetes mientras están en tránsito.

Esta técnica consiste en enviar a una potencial víctima un enlace a una **página maliciosa** o un **sitio legítimo con publicidad maliciosa**, diseñado especialmente para que, cuando lo visite se active la puerta de enlace para abrir cualquier **puerto TCP o UDP** en el equipo de la víctima, evitando las restricciones de puerto basadas en el navegador.

¿Cómo funciona?

La técnica toma ventaja de la **segmentación de paquetes TCP e IP** para ajustar remotamente los límites del paquete, con el fin de utilizarlo para crear un **paquete TCP/UDP** comenzando con un método **SIP (Session Initiation Protocol)** como **REGISTER** o **INVITE**. **SIP** es un protocolo de comunicaciones utilizado para iniciar, mantener y finalizar sesiones multimedia en tiempo real para aplicaciones de mensajería, video y voz.

Es decir, utiliza una combinación de segmentación de paquetes y solicitudes SIP en HTTP con el fin de engañar al mecanismo de seguimiento de conexión de **NAT ALG (Application Level Gateway)** para que abra puertos arbitrarios de conexiones entrantes al cliente.

ALG es un componente de software que se encarga de gestionar protocolos de aplicación específicos, como **SIP** y **FTP (File Transfer Protocol)**.

Con esta técnica de ataque, el atacante "engaña" al NAT haciéndole creer que está viendo un registro SIP legítimo. Eventualmente, hace que NAT abra el puerto en el paquete original enviado por la víctima.

Para lograr esto, se envía una **solicitud HTTP POST** de gran tamaño con un **ID** y un **formulario web oculto** apuntando al servidor de ataque, el cual ejecuta un rastreador de paquetes utilizado para capturar el tamaño de **MTU (Maximum Transmission Unit)**, del paquete, de los encabezados TCP e IP, entre otros datos no especificados. Estos datos de tamaño son posteriormente transmitidos a la víctima a través de un **mensaje POST separado**.

Además, durante esta fase también toma ventaja de la **función de autenticación** en **TURN (Traversal Using Relays around NAT)**, un protocolo utilizado en conjunto con NAT para la retransmisión de medios desde cualquier par a otro cliente en la red. Esta función es utilizada para provocar un desbordamiento de paquetes y la fragmentación de los paquetes IP. En síntesis, el objetivo principal consiste en **desbordar un paquete TCP o UDP** y forzarlo a dividirse en dos para que el paquete de datos SIP esté al comienzo del límite del segundo paquete.

Posteriormente, **se extrae la dirección IP interna de la víctima** utilizando **WebRTC** (framework de código abierto que permite la comunicación en tiempo real en el navegador) en navegadores modernos como **Google Chrome** o **Mozilla Firefox** o

ejecutando un **ataque de tiempo** en puertas de enlace comunes (192.168.*.1; 10.0.0.1 y redes locales).

Finalmente, según lo especificado por el investigador, una vez el cliente obtenga los **datos de tamaño** y la **dirección IP interna**, construye un **formulario web malicioso** encargado de rellenar los datos POST hasta que el paquete se fragmente, momento en el cual el **REGISTER SIP** que contiene la dirección interna será agregado.

La técnica se llevó a cabo utilizando el **router NetGear Nighthawk R700** (CVE-2020-28041) ejecutando la **versión 2.6.36.4** del **kernel de Linux**.

Impacto:

- Un ataque exitoso permitiría a un atacante eludir la protección de la NAT de la víctima y conectarse directamente a cualquier puerto TCP/UDP del equipo, y así exponer servicios previamente protegidos u ocultos, u otros dispositivos de red internos

Recomendaciones:

- Concientizar a los usuarios para identificar enlaces maliciosos, enviados por correo electrónico o servicios de mensajería.
- Desactivar **ALG** del **router/firewall**, en caso de no ser utilizado.
- Estar alerta a las últimas actualizaciones del firmware de los routers, proveídas por el fabricante.
- Restringir los permisos de los usuarios para instalar y ejecutar aplicaciones de software no deseadas. No agregar usuarios al grupo de administradores locales a menos que sea necesario.

Información adicional:

- https://samy.pl/slipstream/
- https://thehackernews.com/2020/11/new-natfirewall-bypass-attack-lets.html
- https://www.redeszone.net/noticias/seguridad/nat-slipstreaming-ataque-evita-firewall/
- https://www.theregister.com/2020/11/02/application_level_gateway_flaw/