Un nuevo vector de ataque distribuido de denegación de servicio (DDoS) ha atrapado a los sistemas Plex Media Server, con el fin de amplificar el tráfico malicioso contra objetivos para desconectarlos.

> *«Los procesos de inicio de Plex sin querer exponen a un respondedor de registro del servicio UPnP Plex a Internet en general, donde se puede abusar para generar ataques DDoS de reflexión/amplificación»,* dijeron los investigadores de NetScout.

Plex Media Server es una biblioteca de medios personal y un sistema de transmisión que se ejecuta en sistemas operativos modernos de Windows, MacOS y Linux, así como variantes personalizadas para plataformas de propósito especial como dispositivos de almacenamiento conectados a la red (NAS) y reproductores de medios digitales. La aplicación de escritorio organiza videos, audio y fotos de la biblioteca de un usuario y de los servicios en línea, lo que permite acceder y transmitir el contenido a otros dispositivos compatibles.

Los ataques DDoS generalmente implican inundar un objetivo legítimo con tráfico de red no deseado que proviene de una gran cantidad de dispositivos que se han acorralado en una botnet, lo que causa efectivamente el agotamiento del ancho de banda y provoca importantes interrupciones de servicio.

Un ataque de amplificación DDoS ocurre cuando un atacante envía una serie de solicitudes especialmente diseñadas a un servidor de terceros que hace que el servidor responda con grandes respuestas a una víctima. Esto se hace falsificando la dirección IP de origen para que parezca que es la víctima en lugar del atacante, lo que genera un tráfico que sobrepasa los recursos de la víctima.

Debido a esto, cuando los terceros responden a la solicitud del atacante, las respuestas se envían al servidor al que se dirige en lugar de al dispositivo atacante que envió la solicitud.

Según Netscout, los servicios de DDoS por alquiler están armando Plex Media Servers para reforzar su infraestructura de ataque, proporcionando de este modo un factor de

amplificación promedio de aproximadamente 4.68.

Plex utiliza el Protocolo Simple de Descubrimiento de Servicios (SSDP) para escanear otros dispositivos multimedia y clientes de transmisión, pero esto da lugar a un problema cuando la sonda localiza un enrutador de acceso a Internet de banda ancha habilitado para SSDP, y en el proceso, expone el registro del servicio Plex directamente en Internet en el puerto UDP 32414.

Por si fuera poco, la compañía de seguridad dijo que identificó alrededor de 27 mil servidores abusivos en Internet hasta ahora.

> *«El impacto colateral de los ataques de reflexión/amplificación PMSSDP es potencialmente significativo para los operadores de acceso a Internet de banda ancha cuyos clientes han expuesto inadvertidamente reflectores/amplificadores PMSSDP a Internet»*, dijeron los investigadores de Netscout, Roland Dobbins y Steinthor Bjarnason.
>
> *«Esto puede incluir la interrupción total o parcial del acceso a Internet de banda ancha del cliente final, así como una interrupción adicional del servicio debido al consumo de capacidad de enlace de acceso/distribución/agregación/núcleo/peering/tránsito».*

Netscout recomienda a los operadores de red filtrar el tráfico dirigido hacia UDP/32414 y deshabilitar SSDP en el equipo de acceso a Internet de banda ancha proporcionado por el operador para mitigar el ataque.

El desarrollo se produce después de que Netscout, a incios de febrero, informara que los servicios DDoS de alquiler están abusando de los servidores Windows Remote Desktop Protocol (RDP) como un vector DDoS de reflexión/amplificación.