Una variante recientemente diseñada del ataque NAT Slipstreaming, puede aprovecharse para comprometer y exponer cualquier dispositivo en una red interna, según las últimas investigaciones.

Detallado por la compañía de seguridad de IoT empresarial Armis, el nuevo ataque (CVE-2020-16043 y CVE-2021-23961), se basa en la técnica previamente divulgada para evitar enrutadores y firewalls, y llegar a cualquier dispositivo no administrado dentro de la red interna desde Internet.

Revelado por primera vez por el investigador de seguridad Samy Kamkar a fines de octubre de 2020, el ataque basado en JavaScript se basaba en atraer a un usuario a visitar un sitio web malicioso para eludir las restricciones de puerto basadas en el navegador y permitir al atacante acceder de forma remota a los servicios TCP/UDP en el dispositivo de la víctima, incluso a los que estaban protegidos por un firewall o NAT.

Aunque el 11 de noviembre de lanzaron mitigaciones parciales para frustrar el ataque en Chrome 87, Firefox 84 y Safari, al impedir las conexiones en el puerto 5060 o 5061, los investigadores de Armis, Ben Seri y Gregory Vishnipolsky, revelaron que *«NAT Slipstreaming 2.0 pone a los dispositivos integrados no administrados en mayor riesgo, al permitir a los atacantes exponer dispositivos ubicados en redes internas, directamente a Internet».*

Los dispositivos vulnerables que podrían estar potencialmente expuestos como consecuencia de este ataque incluyen impresoras de oficina, controladores industriales, cámaras IP y otras interfaces no autenticadas que podrían explotarse una vez que el NAT/firewall sea engañado para abrir tráfico de red al dispositivo de la víctima.

> *«El uso de la nueva variante del ataque NAT Slipstreaming para acceder a este tipo de interfaces desde Internet, puede resultar en ataques que van desde una molestia hasta una sofisticada amenaza de ransomware»,* dijeron los investigadores.

Google, Apple, Mozilla y Microsoft lanzaron parches para los navegadores Chrome (v87.0.4280.141), Safari (v14.0.3), Firefox (v85.0) y Edge (v87.0.664.75) para abordar los nuevos ataques.

Uso de paquetes H.323 para facilitar NAT Slipstreaming

NAT Slipstreaming permite que un mal actor eluda NAT/Firewall y acceda remotamente a cualquier servicio TCP/UDP vinculado a una máquina víctima como resultado de que el objetivo visite un sitio web infectado con malware especialmente diseñado para este propósito.

Particularmente, el código JavaScript malicioso que se ejecuta en el navegador de la víctima extrae la dirección IP interna y aprovecha la segmentación de paquetes TCP/IP para crear grandes balizas TCP/UDP y luego, contrabandear un paquete de Protocolo de Inicio de Sesión (SIP) que contiene la dirección IP interna dentro de una solicitud de salida HTTP Post a través del puerto TCP 5060.

> *«Esto se logra estableciendo cuidadosamente el valor de una conexión TCP controlada por el atacante desde el navegador de la víctima al servidor de un atacante, de forma que un segmento TCP en el 'medio' de la solicitud HTTP sea completamente controlado por el atacante»,* agregaron los investigadores.

Como consecuencia, esto hace que la puerta de enlace de nivel de aplicación NAT (ALG) abra puertos arbitrarios para conexiones entrantes al dispositivo del cliente por medio de la dirección IP interna.

NAT Slipstreaming 2.0 es parecido al ataque mencionado anteriormente en la forma como utiliza el mismo enfoque, pero se basa en el protocolo VoIp H.323 en lugar de SIP para enviar múltiples solicitudes de recuperación al servidor del atacante en el puerto H.323 (1720), lo

que permite al atacante iterar a través de un rango de direcciones IP y puertos, y abrir cada uno de ellos a Internet.

> *«Una solución duradera, desafortunadamente, requeriría cierta revisión de la infraestructura de Internet a la que estamos acostumbrados»*, dijeron los investigadores.
>
> *«Es importante comprender que la seguridad no fue la agenda principal para la creación de NAT, sino que fue principalmente un subproducto del potencial agotamiento de las direcciones IPv4. Los requisitos heredados como las ALG siguen siendo un tema dominante en el diseño de NAT hoy en día, y son la razón principal por la que los ataques de desvío se encuentran una y otra vez»*, agregaron.