Citrix emitió un aviso de emergencia en el que advierte a sus clientes sobre un problema de seguridad que afecta a sus dispositivos de controlador de entrega de aplicaciones (ADC) NetScaler, que los atacantes están abusando para lanzar ataques de denegación de servicio distribuido (DDoS) amplificados contra diversos objetivos.

> *«Un atacante o bots pueden abrumar el rendimiento de la red Citrix ADC, lo que podría conducir al agotamiento del ancho de banda de salida. El efecto de este ataque parece ser más prominente en conexiones con ancho de banda limitado»*, dijo la compañía.

Los ADC son dispositivos de red especialmente diseñados cuya función es mejorar el rendimiento, la seguridad y la disponibilidad de las aplicaciones entregadas a través de la web a los usuarios finales.

El proveedor de servicios de redes y virtualización de escritorio dijo que está monitoreando el incidente y sigue investigando su impacto en Citrix ADC, y agregó que *«el ataque está limitado a una pequeña cantidad de clientes en todo el mundo».*

El problema salió a la luz después de varios informes de un ataque de amplificación DDoS sobre UDP/443 contra dispositivos Citrix (NetScaler) Gateway al menos desde el 19 de diciembre, según Marco Hofmann, administrador de TI de una empresa de software alemana ANAXCO GmbH.

La seguridad de la capa de transporte de datagramas o DTLS se basa en el protocolo de seguridad de la capa de transporte (TLS) que tiene como objetivo proporcionar comunicaciones seguras de una forma que está diseñada para evitar las escuchas, la manipulación o la falsificación de mensajes.

Desde DTLS utiliza la conexión Datagram Protocol (UDP), lo que facilita a un atacante falsificar un datagrama de paquete IP e incluir una dirección IP de origen arbitrario.

Por lo tanto, cuando Citrix ADC se inunda con un flujo abrumador de paquetes DTLS cuyas direcciones IP de origen se falsifican en una dirección IP de la víctima, las respuestas provocadas conducen a una sobresaturación del ancho de banda, creando una condición DDoS.

Citrix está trabajando actualmente para mejorar DTLS para eliminar la susceptibilidad a este ataque, y se espera que se lance un parche el 12 de enero de 2021.

Para determinar si un equipo Citrix ADC es el objetivo del ataque, Cisco recomienda vigilar el volumen del tráfico saliente en busca de anomalías o picos significativos.

Los clientes afectados por el ataque, mientras tanto, pueden desactivar DTLS mientras esté pendiente una solución permanente de Citrix ejecutando el siguiente comando en Citrix ADC: *«set vpn vserver -dtls OFF»*.