Citrix finalmente comenzó a implementar parches de seguridad para una vulnerabilidad crítica en el software ADC y Gateway, que los piratas informáticos comenzaron a explotar en la naturaleza a inicios de este mes, luego de que la compañía anunciara la existencia del problema sin lanzar ninguna solución permanente.

Este corto período de tiempo en el que no existieron parches para las vulnerabilidades, los hackers no perdieron el tiempo y estuvieron comprometiendo cientos de sistemas Citrix ADC y Gateway expuestos a Internet.

La vulnerabilidad, registrada como CVE-2019-19781, es un problema de recorrido de ruta que podría permitir a los atacantes remotos no autenticados ejecutar código arbitrario en distintas versiones de Citrix ADC y productos Gateway, así como en las dos versiones anteriores de Citrix SD-WAN- WANOP.

Calificado como muy crítico con el puntaje básico de CVSS v3.1 9.8, el problema fue descubierto por Mikhail Klyuchnikov, un investigador de seguridad cibernética de Positive Technologies, quién informó sobre el fallo de forma responsable a Citrix a inicios de diciembre de 2019.

La vulnerabilidad está siendo explotada activamente desde la semana pasada por muchos hackers y atacantes individuales, gracias al lanzamiento público de distintos códigos de explotación de pruebas de concepto.

Según los expertos en seguridad cibernética, a partir de hoy, existen más de 15 mil servidores Citrix ADC y Gateway vulnerables de acceso público que los atacantes pueden explotar en cualquier momento para atacar redes empresariales.

Expertos de FireEye encontraron una campaña de ataque en la que alguien comprometía los ADC Citrix vulnerables para instalar una carga útil nunca antes vista, denominada *«NotRobin»*, que escanea los sistemas en busca de criptomineros y malware desplegados por otros atacantes potenciales y los elimina para mantener el acceso exclusivo de puerta trasera.

> *«Este actor explota los dispositivos NetScaler utilizando CVE-2019-19781 para ejecutar comandos de shell en el dispositivo comprometido»*, dijo FireEye.
>
> *«FireEye cree que el actor detrás de NotRobin ha estado comprometiendo de forma oportunista los dispositivos NetScaler, posiblemente para prepararse para una próxima campaña».*

La semana pasada, Citrix anunció una línea de tiempo, prometiendo lanzar actualizaciones de firmware parcheadas para todas las versiones compatibles del software ADC y Gateway antes de finales de enero de 2020, como se muestra en la siguiente tabla:

Como parte de su primer lote de actualizaciones, Citrix lanzó hoy los parches permanentes para ADC versiones 11.1 y 12.0 que también se aplican a *«ADC Gateway VPX alojados en ESX, Hyper-V, KVM, XenServer, Azure, AWS, GCP o en un Citrix ADC Service Delivery Appliance (SDX)».*

> *«Es necesario actualizar todas las instalaciones Citrix ADC y Citrix Gateway 11.1 (MPX o VPX) para construir 11.1.63.15 para instalar las correcciones de vulnerabilidad de seguridad. Es necesario actualizar todas las instancias Citrix ADC y Citrix Gateway 12.0 (MPX o VPX) a compilar 12.0.63.13 para instalar las correcciones de vulnerabilidad de seguridad»,* dijo Citrix en su aviso.
>
> *«Instamos a los clientes a instalar estas soluciones de inmediato. Si aún no lo ha hecho, debe aplicar la mitigación suministrada anteriormente a las versiones ADC 12.1, 13, 10.5 y SD-WAN WANOP versiones 10.2.16 y 11.0.3, hasta que las soluciones para esas versiones estén disponibles».*

La compañía también advirtió que los clientes con múltiples versiones de ADC en producción deben aplicar la versión correcta del parche a cada sistema por separado.

Además de instalar parches disponibles para versiones compatibles y aplicar la mitigación recomendada para sistemas sin parches, también se recomienda a los administradores de Citrix ADC que supervisen los registros de sus dispositivos para detectar ataques.