Este viernes, varios grupos de piratas informáticos lanzaron públicamente códigos de explotación de prueba de concepto armado para una vulnerabilidad de ejecución remota de código recientemente revelada en los productos NetScaler ADC y Gateway de Citrix, que podrían permitir que cualquiera los aproveche para tomar el control total sobre posibles objetivos empresariales.

Antes de las fiestas decembrinas, Citrix anunció que su Citrix Application Delivery Controller (ADC) y Citrix Gatewat son vulnerables a una falla transversal de ruta crítica (CVE-2019-19781), que podría permitir que un hacker no autenticado realice la ejecución de código arbitrario en servidores vulnerables.

Citrix confirmó que la falla afecta a todas las versiones compatibles del software, que incluyen:

- Citrix ADC y Citrix Gateway versión 13.0, todas las compilaciones compatibles
- Citrix ADC y NetScaler Gateway versión 12.1, todas las compilaciones compatibles
- Citrix ADC y NetScaler Gateway versión 12.0, todas las compilaciones compatibles
- Citrix ADC y NetScaler Gateway versión 11.1, todas las compilaciones compatibles
- Citrix NetScaler ADC y NetScaler Gateway versión 10.5, todas las compilaciones compatibles

La compañía hizo la divulgación sin publicar parches de seguridad para software vulnerable. En cambio, Citrix ofreció mitigación para ayudar a los administradores a proteger sus servidores contra posibles ataques remotos, e incluso en este momento, no existen parches disponibles a 23 días de hacerse público el problema.

Por medio de los ataques cibernéticos contra servidores vulnerables, se vieron por primera vez en la naturaleza la semana pasada cuando los piratas informáticos desarrollaron exploits privados luego de la información de mitigación de ingeniería inversa, el lanzamiento público de PoC armado ahora facilitaría a los script kiddies poco calificados lanzar ataques cibernéticos contra organizaciones vulnerables.

Según Shodan, hasta este momento existen poco más de 125,400 servidores Citrix ADC o Gateway accesibles públicamente y pueden explotarse durante la noche si no se desconectan o protegen mediante la mitigación disponible.

Antes de aplicar la mitigación recomendada, sería importante que los administradores de Citrix ADC supervisen los registros de sus dispositivos para detectar ataques.