Citrix está emitiendo una advertencia sobre la explotación de una vulnerabilidad crítica recientemente divulgada en los dispositivos NetScaler ADC y Gateway que podría dar lugar a la exposición de información confidencial.

Identificada como CVE-2023-4966 (puntuación CVSS: 9.4), esta vulnerabilidad afecta a las siguientes versiones compatibles:

- NetScaler ADC y NetScaler Gateway 14.1 antes de la versión 14.1-8.50
- NetScaler ADC y NetScaler Gateway 13.1 antes de la versión 13.1-49.15
- NetScaler ADC y NetScaler Gateway 13.0 antes de la versión 13.0-92.19
- NetScaler ADC y NetScaler Gateway 12.1 (actualmente en estado de fin de vida)
- NetScaler ADC 13.1-FIPS antes de la versión 13.1-37.164
- NetScaler ADC 12.1-FIPS antes de la versión 12.1-55.300, y
- NetScaler ADC 12.1-NDcPP antes de la versión 12.1-55.300

No obstante, para que se produzca la explotación, se requiere que el dispositivo esté configurado como un Gateway (servidor virtual VPN, ICA Proxy, CVPN, RDP Proxy) o como un servidor virtual de autorización y contabilidad (AAA).

A pesar de que los parches para esta vulnerabilidad se lanzaron el 10 de octubre de 2023, Citrix ha actualizado su advertencia para destacar que *«se han observado ataques de CVE-2023-4966 en dispositivos que no han sido protegidos».*

Mandiant, propiedad de Google, en su propia alerta publicada el martes, informó que identificó la explotación de día cero de esta vulnerabilidad en la naturaleza a partir de finales de agosto de 2023.

> *«Una explotación exitosa podría dar lugar a la capacidad de tomar control de sesiones autenticadas existentes, eludiendo así la autenticación de múltiples factores u otros requisitos de autenticación sólida»*, afirmó la firma de inteligencia de amenazas.

> *«Estas sesiones podrían persistir incluso después de la implementación de la actualización para mitigar CVE-2023-4966».*

Mandiant también indicó que detectó casos de secuestro de sesiones en los que los datos de la sesión fueron robados antes de la aplicación del parche y posteriormente utilizados por un actor de amenazas no identificado.

> *«El secuestro de sesiones autenticadas podría, entonces, dar lugar a un acceso adicional, dependiendo de los permisos y el alcance de acceso otorgados a la identidad o sesión»,* agregó.

> *«Un actor de amenazas podría aprovechar este método para obtener credenciales adicionales, avanzar lateralmente y acceder a recursos adicionales dentro del entorno».*

No se ha determinado quién está detrás de estos ataques, pero se informa que la campaña ha tenido como objetivo a servicios profesionales, organizaciones tecnológicas y gubernamentales.

Dado el abuso activo de esta vulnerabilidad y el hecho de que los errores de Citrix se han convertido en un enfoque preferido de los actores de amenazas, es fundamental que los usuarios actualicen rápidamente a la versión más reciente para mitigar posibles amenazas.

> *«Las organizaciones deben hacer más que simplemente aplicar el parche; también deben finalizar todas las sesiones activas. Aunque no se trata de una vulnerabilidad de ejecución remota de código, les insto a dar prioridad a la implementación de este parche debido a la explotación activa y a la gravedad de la vulnerabilidad»,* comentó Charles Carmakal, CTO de Mandiant.