Miles de puntos finales de Citrix Application Delivery Controller (ADC) y Gateway siguen siendo vulnerables a dos vulnerabilidades de seguridad críticas reveladas por la compañía en los últimos meses.

Los problemas en cuestión son CVE-2022-27510 y CVE-2022-27518 (puntaje CVSS: 9.8), que fueron abordados por el proveedor de servicios de virtualización el 8 de noviembre y el 13 de diciembre de 2022, respectivamente.

Mientras que CVE-2022-27510 se relaciona con una omisión de autenticación que podría explotarse para obtener acceso no autorizado a las capacidades del usuario de Gateway, CVE-2022-27518 se refiere a un error de ejecución de código remoto que podría permitir la toma de control de los sistemas afectados.

Citrix y la Agencia de Seguridad Nacional de Estados Unidos (NSA), a inicios del mes, advirtieron que CVE-2022-27518 está siendo explotado activamente por actores de amenazas, incluyendo el grupo patrocinado por el estado APT5 vinculado a China.

Ahora, según un nuevo análisis del equipo de investigación Fox-IT de NCC Group, miles de servidores Citrix con acceso a Internet aún no tienen parches, lo que los convierte en un objetivo atractivo para los equipos de hacking.

Esto incluye más de 3500 servidores Citrix ADC y Gateway que ejecutan la versión 12.1-65.21 que son susceptibles a CVE-2022-27518, así como más de 500 servidores que ejecutan 12.1-63.22 que son vulnerables a ambas fallas.

La mayoría de los servidores, que ascienden a no menos de 5000, ejecutan 13.0-88.14, una versión que es inmune a CVE-2022-27510 y CVE-2022-27518.

Un desglose por países muestra que más del 40% de los servidores ubicados en Dinamarca, los Países Bajos, Austria, Alemania, Francia, Singapur, Australia, el Reino Unido y Estados Unidos, de casi 550 servidores han sido parcheados.

Fox-IT dijo que pudo deducir la información de la versión de un valor hash similar a MD5 presente en la respuesta HTTP de la URL de inicio de sesión (es decir, «*ns_gui/vpn/index.html*»)y asignarlo a sus respectivas versiones.