Cerca de 2,000 instancias de Citrix NetScaler han sido infiltradas con una puerta trasera al aprovechar una vulnerabilidad crítica recientemente divulgada como parte de un ataque a gran escala.

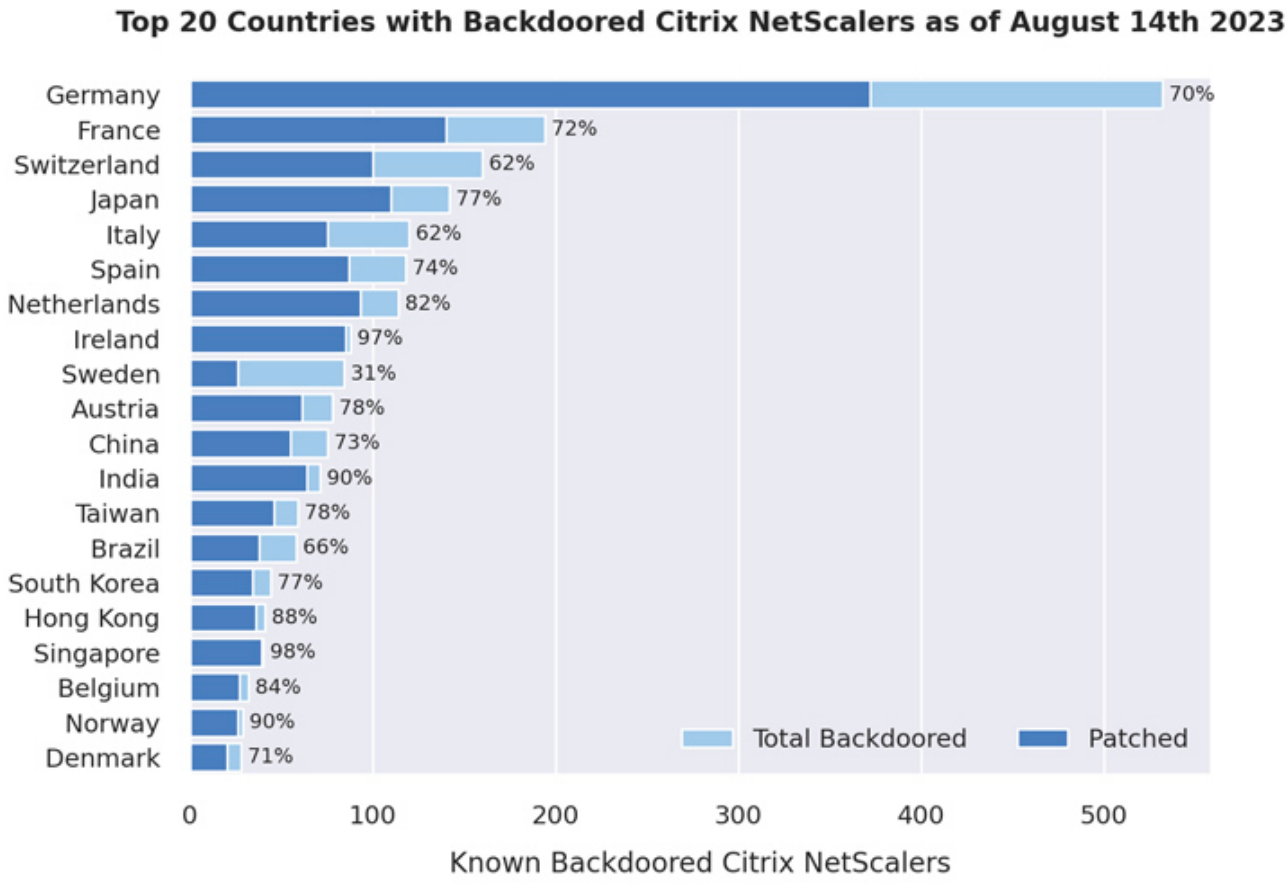
> *«Un adversario parece haber explotado CVE-2023-3519 de forma automatizada, insertando shell webs en NetScalers vulnerables para obtener acceso persistente»*, indicó NCC Group en un comunicado emitido el martes.

> *«El adversario puede ejecutar comandos arbitrarios con este shell web, incluso cuando un NetScaler ha sido parcheado y/o reiniciado.»*

CVE-2023-3519 se refiere a una vulnerabilidad crítica de inyección de código que afecta a los servidores NetScaler ADC y Gateway, lo cual podría conducir a la ejecución remota de código sin autenticación. Citrix corrigió esto el mes pasado.

Este acontecimiento se produce una semana después de que la Fundación Shadowserver declarara haber identificado cerca de 7,000 instancias vulnerables y sin parchear de NetScaler ADC y Gateway en línea, y que la falla está siendo aprovechada para insertar shell webs PHP en servidores vulnerables para acceder de forma remota.

Un análisis de seguimiento realizado por NCC Group ha revelado que todavía hay 1,828 servidores NetScaler con una puerta trasera, de los cuales aproximadamente 1,248 ya han sido parcheados contra la falla.



> *«Esto indica que, si bien la mayoría de los administradores eran conscientes de la vulnerabilidad y han parcheado sus NetScalers a una versión no vulnerable, no se han revisado (adecuadamente) en busca de señales de explotación exitosa»,* explicó la compañía.

En conjunto, se han hallado hasta 2,491 shell webs en 1,952 dispositivos NetScaler diferentes. La mayoría de las instancias comprometidas se encuentran en Alemania, Francia, Suiza, Japón, Italia, España, los Países Bajos, Irlanda, Suecia y Austria.

Aparte del enfoque en Europa, otro aspecto destacable es que, aunque Canadá, Rusia y

Estados Unidos tenían miles de servidores NetScaler vulnerables a finales del mes pasado, no se encontraron shell webs en ninguno de ellos.

Se calcula que la campaña de explotación masiva ha infiltrado el 6.3% de las 31,127 instancias de NetScaler que eran susceptibles a CVE-2023-3519 hasta el 21 de julio de 2023.

La revelación también llega en un momento en que Mandiant ha lanzado una herramienta de código abierto para ayudar a las organizaciones a escanear sus dispositivos Citrix en busca de pruebas de actividad posterior a la explotación relacionada con CVE-2023-3519.