BEACON LAB
C S I R T

CYBOLT

Alert Bulletin

Bulletin N.: 55
Publication Date: 30/06/2025
Subject: Alerta 2025-55 Vulnerabilidades críticas en NetScaler ADC y NetScaler Gateway
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **Citrix NetScaler ADC** (antes Citrix ADC) y **Citrix NetScaler Gateway** (antes Citrix Gateway)
  - NetScaler ADC/Gateway 14.1 anteriores a 14.1-43.56
  - NetScaler ADC/Gateway 13.1 anteriores a 13.1-58.32
  - NetScaler ADC 13.1-FIPS/NDcPP anteriores a 13.1-37.235
  - NetScaler ADC 12.1-FIPS anteriores a 12.1-55.328

Descripción

Recientemente, el Cloud Software Group reveló dos vulnerabilidades **críticas** en sus productos **Citrix NetScaler ADC (antes Citrix ADC),** dispositivo para optimizar, asegurar y escalar la entrega de aplicaciones web y móviles (balanceador), **y Citrix NetScaler Gateway (antes Citrix Gateway),** componente orientado a proporcionar acceso remoto seguro a aplicaciones, escritorios y datos corporativos**,** identificadas como **CVE-2025-6543** y **CVE-2025-5777**, permiten a un atacante **remoto y no autenticado** leer fuera de los límites de memoria y extraer tokens de inicio de sesión y hashes criptográficos para secuestrar sesiones y eludir MFA, así como generar ataques de denegación de servicios en entornos productivos.

Ambas vulnerabilidades han recibido **calificaciones críticas**, de **CVSS 9.2 y 9.3** respectivamente, lo que las convierte en amenazas de alto impacto para las organizaciones que utilizan estas soluciones de NetScaler en entornos de autenticación, control de acceso y monitoreo de identidad.

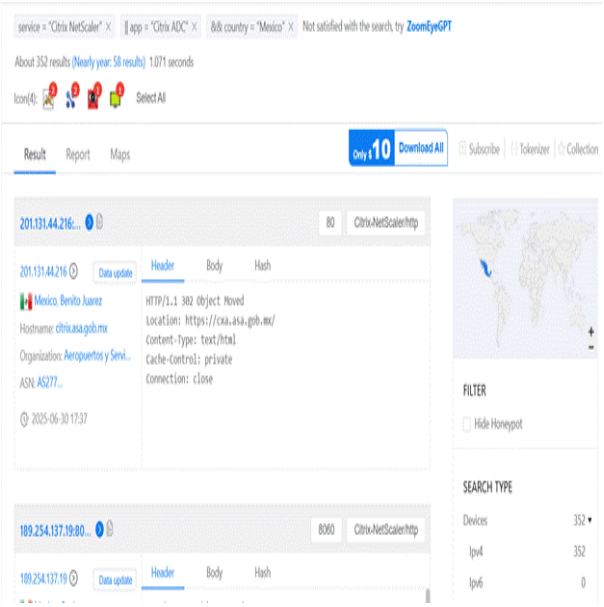
- **CVE-2025-5777 (también conocida como "CitrixBleed 2")**

Esta vulnerabilidad es un fallo de validación de entrada que permite a un atacante remoto y no autenticado leer fuera de los límites de memoria del dispositivo, exponiendo tokens de sesión y hashes criptográficos usados para MFA. Su explotación posibilita el secuestro de sesiones válidas y eludir controles de autenticación, obteniendo un puntaje CVSS v4.0 de 9.3 (Crítico).

- **CVE-2025-6543**

Es una vulnerabilidad de desbordamiento de memoria que ocurre durante el procesamiento de paquetes de autenticación y AAA, permitiendo corromper estructuras internas y provocar Denegación de Servicio (DoS). Con un CVSS v4.0 de 9.2 (Crítico), ya se han registrado incidentes de interrupción de servicio en entornos productivos

En **México**, se identificaron al menos 352 dispositivos ADC y Gateway de NetScaler expuestos en Internet.



Solución:

Se recomienda a los clientes actualizar a los builds 14.1-43.56 y 14.1-47.46 (o superiores) y a 13.1-58.32 y 13.1-59.19 (o superiores), incluyendo en entornos FIPS/NDcPP las versiones mínimas 12.1-55.328 y 13.1-37.236; una vez completada la actualización en todos los nodos, ejecute kill icaconnection -all y kill pcoipConnection -all para invalidar sesiones antiguas potencialmente comprometidas, y paralelamente restrinja el acceso a los VIP de Gateway y los servidores AAA sólo a redes de gestión confiables, deshabilitando temporalmente cualquier servidor virtual innecesario hasta verificar que el parche está correctamente aplicado.

Para obtener instrucciones sobre cómo actualizar un dispositivo, consulte las Guías de actualización en la página de soporte de Netscaler en el siguiente enlace:

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788

Información adicional:

- https://www.netscaler.com/blog/news/netscaler-critical-security-updates-for-cve-2025-6543-and-cve-2025-5777/
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788
- https://thehackernews.com/2025/06/citrix-releases-emergency-patches-for.html