Boletín de alerta

Boletín Nro.: 110
Fecha de publicación: 29/09/2026
Tema: Alerta 2026-110 Explotación Activa deVulnerabilidades 0- Day en Citrix
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Configuración / condición	Vulnerabilidades
Citrix NetScaler ADC	Configuración predeterminada	CVE□2026□8771
Citrix NetScaler Gateway	Configuración predeterminada	CVE□2026□8771
Citrix NetScaler ADC	DTLS habilitado	CVE□2026□8772
Citrix NetScaler Gateway	DTLS habilitado, normalmente activo por defecto en VPN virtual servers	CVE□2026□8772
NetScaler ADC / Gateway 12.1 y 13.0	Sin soporte / End of Life	No hay parche; requiere migración a una release soportada

Descripción

Se ha publico dos vulnerabilidades Zero Days en **NetScaler ADC** y **Citrix NetScaler Gateway**: **CVE□2026□ 88771 (CVSSv4 9.5)** y **CVE□2026□8772 (CVSSv4 9.5)**. Ambas permiten a atacantes remotos no autenticados obtener **ejecución remota de código (RCE)** en appliances vulnerables; la primera afecta despliegues con configuración predeterminada y la segunda requiere que **DTLS** esté habilitado, una función activada por defecto en servidores virtuales VPN. Citrix confirmó que se ha observado explotación de **CVE□2026□8771** y **CVE□2026□8772** en despliegues NetScaler no mitigados.

A continuación se detallan las vulnerabilidades:

- **CVE□2026□8771 — validación de entrada incorrecta / RCE preautenticada**

CVE□2026□8771 es una vulnerabilidad de ejecución remota de código causada por validación insuficiente de entradas (**CWE□20**) en NetScaler ADC y NetScaler Gateway. Tiene una puntuación **CVSS v4.0 de 9.5** y afecta a todos los despliegues vulnerables, incluso con la configuración predeterminada; no requiere

habilitar una función adicional.

Un atacante remoto no autenticado puede enviar solicitudes especialmente diseñadas al appliance y ejecutar comandos arbitrarios. La falla requiere conectividad de red hacia el servicio vulnerable, pero no exige credenciales, interacción de usuario ni una configuración especial distinta de la configuración estándar del producto.

- **CVE-2026-38772 — desbordamiento de memoria / RCE o DoS mediante DTLS**

CVE-2026-38772 es una vulnerabilidad de desbordamiento de memoria (**CWE-119**) que puede derivar en ejecución remota de código o denegación de servicio. También tiene **CVSS v4.0 9.5**, pero su exposición requiere que **DTLS esté habilitado** en NetScaler ADC o Gateway.

DTLS está habilitado de forma predeterminada en los **VPN virtual servers**, por lo que todos los appliances que ofrezcan acceso VPN deben ser tratados como potencialmente afectados hasta verificar la configuración y aplicar el parche. La complejidad de ataque indicada por Citrix es alta, pero la explotación activa eleva la urgencia de la remediación.

Solución

La solución definitiva es instalar una de las versiones corregidas de Citrix NetScaler:

- **14.1-73.37 o posterior** para NetScaler ADC y Gateway 14.1.
- **13.1-64.23 o posterior** para NetScaler ADC y Gateway 13.1.
- **14.1-73.37 FIPS o posterior** para NetScaler ADC 14.1-FIPS.
- **13.1-37.279 o posterior** para NetScaler ADC 13.1-FIPS y 13.1-NDcPP.

Los appliances en ramas 12.1 y 13.0 deben migrar a una release soportada, ya que no existe una actualización de seguridad disponible para esas versiones.

Producto / rama	Versión mínima corregida
NetScaler ADC y NetScaler Gateway 14.1	14.1-73.37 o posterior
NetScaler ADC y NetScaler Gateway 13.1	13.1-64.23 o posterior
NetScaler ADC 14.1-FIPS	14.1-73.37 FIPS o posterior
NetScaler ADC 13.1-FIPS	13.1-37.279 o posterior
NetScaler ADC 13.1-NDcPP	13.1-37.279 o posterior
NetScaler ADC / Gateway 12.1 y 13.0	Migrar a versión soportada; no reciben actualizaciones de seguridad

Antes de actualizar, NetScaler recomienda verificar espacio libre, realizar copia de la configuración, validar prerrequisitos y descargar el firmware aplicable desde el portal oficial. Para una actualización segura, la documentación indica disponer de al menos **7 GB libres en /var** y **200 MB en /flash** para un appliance

standalone; las validaciones previas deben completarse sin errores antes de iniciar la instalación.

Para dispositivos **standalone**, el flujo recomendado es:

1. Guardar la configuración actual con save config.
2. Respaldar el archivo /nsconfig/ns.conf y confirmar espacio disponible.
3. Descargar y cargar el paquete de firmware correspondiente a la rama instalada.
4. Ejecutar las validaciones previas desde **System > System Upgrade** en la GUI, o ./installns –pre_check desde CLI.
5. Instalar la actualización y reiniciar cuando el proceso lo solicite.
6. Confirmar la build instalada, la salud del appliance, los *virtual servers*, autenticación, VPN, DTLS, balanceo y aplicaciones publicadas.

Para pares en **High Availability (HA)**, NetScaler recomienda actualizar primero el **nodo secundario**, forzar el *failover* y luego actualizar el nodo que era primario. Esto minimiza el impacto y permite mantener continuidad del servicio durante la actualización.

No existe un *workaround* publicado por Citrix que elimine por completo CVE□2026□8771 o CVE□2026□8772; actualizar a una build corregida es la única remediación definitiva. Deshabilitar DTLS puede reducir temporalmente la exposición a CVE□2026□8772 cuando no afecte la operación, pero no protege frente a CVE□2026□8771.

Enlaces oficiales para ayudar en el proceso de actualización:

- https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-before-you-begin.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-standalone-appliance.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-ha-pair.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/pre-upgrade-validation-checks.html

Información adicional:

- https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-exploited-citrix-flaws-by-wednesday/
- https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html