Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CITRIX CORRIGE TRES VULNERABILIDADES CRÍTICAS EN NETSCALER: UNA DE ELLAS YA ESTÁ SIENDO EXPLOTADA

26/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Citrix ha publicado actualizaciones críticas para NetScaler ADC y NetScaler Gateway tras descubrir tres vulnerabilidades graves que afectan a sus dispositivos. Una de ellas, identificada como CVE-2025-7775, ya está siendo explotada activamente en entornos reales, lo que incrementa de forma significativa el nivel de riesgo para las organizaciones que aún no han aplicado las correcciones.

Estas fallas podrían permitir a los atacantes ejecutar código de manera remota, interrumpir servicios esenciales mediante denegación de servicio o incluso acceder indebidamente a la interfaz de administración de NetScaler. Ante la ausencia de soluciones temporales, Citrix recomienda actualizar de inmediato a las versiones seguras para proteger la infraestructura crítica de las empresas.

CITRIX CORRIGE TRES VULNERABILIDADES CRÍTICAS EN NETSCALER: UNA DE ELLAS YA ESTÁ SIENDO EXPLOTADA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_26_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/08/2025
Es día cero (0 day):	No

RESUMEN

Citrix ha publicado actualizaciones de seguridad para NetScaler ADC y NetScaler Gateway, solucionando tres vulnerabilidades graves. Una de ellas (CVE-2025-7775) ya está siendo explotada de manera activa, lo que aumenta la urgencia de aplicar los parches correspondientes.

Vulnerabilidades detectadas

Citrix ha corregido las siguientes fallas de seguridad:

- **CVE-2025-7775 (CVSS 9.2)**
  Desbordamiento de memoria que puede derivar en ejecución remota de código o denegación de servicio (DoS).
  - Requiere que NetScaler esté configurado como Gateway (VPN, ICA Proxy, CVPN, RDP Proxy) o ciertos virtual servers con servicios IPv6 habilitados.
  - Esta es la vulnerabilidad que ya se encuentra en explotación activa.
- **CVE-2025-7776 (CVSS 8.8)**
  Otro desbordamiento de memoria que ocasiona comportamiento impredecible y DoS.
  - Afecta principalmente a instancias configuradas como Gateway con PCoIP Profile.
- **CVE-2025-8424 (CVSS 8.7)**
  Fallo de control de acceso en la interfaz de administración de NetScaler.
  - Requiere acceso al NSIP, Cluster Management IP, GSLB Site IP local o SNIP con permisos de administración.

Versiones seguras disponibles

Citrix urge a sus clientes a actualizar de inmediato a las siguientes versiones para mitigar los riesgos:

- 14.1-47.48 o superior
- 13.1-59.22 o superior
- 13.1-FIPS/NDcPP 13.1-37.241 o superior
- 12.1-FIPS/NDcPP 12.1-55.330 o superior

La compañía ha señalado que no existen soluciones temporales o workarounds disponibles, por lo que la actualización inmediata es la única medida efectiva.

Riesgo empresarial

El hecho de que una de estas vulnerabilidades ya esté siendo explotada en entornos reales representa un riesgo crítico para las organizaciones que utilizan NetScaler en funciones de VPN, balanceo de carga o acceso remoto. Un atacante podría obtener control del sistema, interrumpir servicios esenciales o acceder a datos sensibles.

Recomendaciones para las empresas

1. Actualizar sin demora las versiones vulnerables de NetScaler a las ediciones corregidas.
2. Revisar los registros y monitorear actividad anómala, especialmente en appliances configurados como Gateway.
3. Restringir el acceso a la interfaz de administración únicamente desde redes seguras y controladas.

Conclusión

Las vulnerabilidades de Citrix NetScaler se han convertido en un objetivo habitual para los actores de amenazas debido a su rol crítico en entornos empresariales. Ante la confirmación de explotación activa de CVE-2025-7775, las organizaciones deben actuar con rapidez y aplicar los parches de seguridad para reducir al mínimo la superficie de ataque.

NOTICIA COMPLETA

https://devel.group/blog/citrix-corrige-tres-vulnerabilidades-criticas-en-netscaler-una-de-ellas-ya-esta-siendo-explotada/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/