Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CITRIX NETSCALER BAJO ATAQUE: EL NCSC HOLANDÉS CONFIRMA EXPLOTACIÓN EN SECTORES CRÍTICOS

13/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente se alertó sobre ciberataques que están explotando una vulnerabilidad de severidad crítica, en dispositivos Citrix NetScaler ADC y Gateway, esta fue identificada como CVE-2025-6543.

CITRIX NETSCALER BAJO ATAQUE: EL NCSC HOLANDÉS CONFIRMA EXPLOTACIÓN EN SECTORES CRÍTICOS

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

ID de alerta:	DSOC-CERT_2025_08_13_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente se alertó sobre ciberataques que están explotando una vulnerabilidad de severidad crítica, en dispositivos Citrix NetScaler ADC y Gateway, esta fue identificada como CVE-2025-6543.

¿En qué consiste?

Es un fallo de tipo desbordamiento de memoria (buffer overflow) que puede alterar el flujo de control del sistema y causar denegación de servicio DoS.

Se presenta cuando los dispositivos están configurados como Gateway (VPN virtual server, ICA Proxy, RDP Proxy, CVPN) o como servidores AAA.

Versiones afectadas

- NetScaler ADC y Gateway 14.1, versiones anteriores a 14.1-47.46
- NetScaler ADC y Gateway 13.1, versiones anteriores a 13.1-59.19
- NetScaler ADC 13.1-FIPS y 13.1-NDcPP, versiones anteriores a 13.1-37.236

Las versiones 12.1 y 13.0 ya no son soportadas y no recibirán parches, por lo que siguen siendo totalmente vulnerables. Se recomienda actualizar a versiones soportadas cuanto antes.

¿Cómo funciona?

Para tener una mejor visualización de la vulnerabilidad podemos imaginar a Citrix NetScaler como un guardia de seguridad que resguarda una empresa (La red) y su trabajo es revisar lo que entra y sale (Datos de usuarios, conexiones VPN, etc.)

La vulnerabilidad CVE-2025-6543 es como si nuestro guardia tuviera un cuaderno para anotar la información que ve, pero su cuaderno es pequeño, entonces un cibercriminal le entrega más información de la que cabe en su cuaderno.

Como nuestro guardia no puede manejar el exceso de datos, la información que no logra recopilar se desborda y se mete en otros lugares de la memoria.

Esto abre una oportunidad para que el cibercriminal cambie lo que el guardia hace (controlar el flujo del programa) o incluso causar que nuestro guardia se desmaye

(provocar una denegación de servicio)

Si el NetScaler está en modo Gateway o AAA, el impacto es mayor porque es el punto que conecta usuarios externos con la red interna.

Explotación y alcance

- La vulnerabilidad fue explotada como zero-day desde principios de mayo de 2025, antes de que Citrix lanzara el parche en junio.
- El ataque incluyó borrado de evidencia para dificultar investigaciones forenses.

RECOMENDACIONES

- Actualizar inmediatamente Citrix NetScaler ADC y Gateway a versiones parcheadas (p.ej., versiones posteriores a 14.1-47.46 y 13.1-59.19).
- Restablecer sesiones establecidas en los dispositivos, ya que también es necesario, según el NCSC-NL.
- En caso de detectar actividad sospechosa, contactar al CSIRT local (equipo de respuesta a incidentes) para asistencia inmediata.

NOTICIA COMPLETA

https://devel.group/blog/citrix-netscaler-bajo-ataque-el-ncsc-holandes-confirma-explotacion-en-sectores-criticos/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

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