Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVAS FALLAS EN NETSCALER PERMITEN ROBO DE TOKENS Y CONTROL REMOTO

25/ 06 / 2025

CONTENIDO

INTRODUCCIÓN

Citrix ha emitido una alerta crítica tras descubrir dos vulnerabilidades severas en sus dispositivos NetScaler ADC y Gateway, identificadas como **CVE-2025-5777** y **CVE-2025-5349**. Estas fallas permiten a atacantes remotos exfiltrar información sensible directamente desde la memoria del sistema o eludir controles de acceso a la interfaz administrativa, sin necesidad de autenticación previa.

NUEVAS FALLAS EN NETSCALER PERMITEN ROBO DE TOKENS Y CONTROL REMOTO

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

ID de alerta:	DSOC-CERT_2025_06_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	25/06/2025
Es día cero (0 day):	No

RESUMEN

Se identifico recientemente dos vulnerabilidades nuevas CVE-2025-5349 y CVE-2025-5777 para NetScaler y NetSacler Gateway.

CVE-2025-5349

La vulnerabilidad se trata de una falla de control de acceso en la interfaz de gestión (Management Interface) para los servicios de NetScaler y NetScaler Gateway. Esta permite que un atacante que posee acceso a direcciones internas como NSIP, IP de gestión de clúster o IP local de GSLB eludir restricciones fijas em esa interfaz.

Cabe recalcar que la vulnerabilidad solo puede ser explotada si el atacante tiene acceso a IPs en propiedad de NetScaler, dispositivo o direcciones IP de administrador del clúster.

Se le asigno una criticidad de CVSS: 8.7

¿Cómo funciona?

Funcionan aprovechándose de las interfaces dedicadas para la administración como: NSIP, NetScaler IP o la IP de administración de clúster.

Lo que deberías de hacer las interfaces es poder restringir algunas funciones administrativas, esto únicamente al tráfico autorizado o previamente autenticado.

Aquí es donde se encuentra la vulnerabilidad, debido a una configuración débil en el firmware afectado, algunas solicitudes enviadas desde direcciones internas pueden evadir estas restricciones.

Para esto no se requiere de una autenticación previa, esto quiere decir que, si un atacante posee acceso de red a alguna de estas IPs internas, podrías ejecutar funciones acciones que deberían de estar bloqueadas o requerir de privilegios más elevados.

Ejemplo – Simulación lógica de vulnerabilidad

```python

# Lista de IPs "internas autorizadas" según NetScaler (NSIP, CLIP, GSLB IP)
ip_autorizadas = ["192.168.0.1", "10.1.1.1", "172.16.5.10"]

# Función vulnerable que simula el acceso a funciones administrativas
def acceder_interfaz_administrativa(ip_origen):
    print(f"\nSolicitud desde: {ip_origen}")

    # Verificación incorrecta que permite acceso sin autenticar si la IP es interna
    if ip_origen in ip_autorizadas:
        print(" ¡Controles de acceso evadidos!")
        ejecutar_funcion_administrativa()
    else:
        print(" Acceso denegado. Controles de acceso aplicados.")

# Función administrativa que debería estar protegida
def ejecutar_funcion_administrativa():
    print(" Función administrativa ejecutada (configuración modificada).")

# Simulación de solicitudes
ips_que_prueban = [
    "192.168.0.1",   # IP interna (NSIP) -> acceso concedido sin autenticación
    "203.0.113.5",   # IP externa -> acceso denegado
    "10.1.1.1",      # IP local permitida -> acceso concedido
    "8.8.8.8"        # IP pública -> acceso denegado
]

for ip in ips_que_prueban:
    acceder_interfaz_administrativa(ip)

```

CVE-2025-5777

Esta vulnerabilidad es clasificada como fallo de lectura fuera de límites esto debido a entradas insuficientes de validación, esto permite al atacante obtener datos importantes directamente de la memoria del dispositivo.

Es importante recalcar que esta vulnerabilidad es igual a una ya conocida como: CritixBleed (CVE-2023-4966)

Se le asigno una criticidad de CVSS: 9.3

¿Cómo funciona?

Lo principal es que el atacante conozca o detecte un dispositivo NetScaler configurado como Gateway (configurados como puerta de enlace) como: VPN, RDP, proxy, AAA, etc.

Este envía una solicitud malformada especialmente para el servicio Gateway expuesto en la red.

Debido a que no se tiene una validación adecuada, la solicitud provoca una lectura fuera de los limites autorizados de la memoria.

Lo que conlleva a que el atacante puede obtener tokens de sesión validos o algún tipo de información sensible alojada en la memoria.

Con estos tokens el atacante puede reproducir sesiones legítimas evitando autenticaciones, incluyendo MFA.

Ejemplo – Simulación lógica de vulnerabilidad

```python
# Memoria simulada del servidor (contiene tokens de usuarios conectados)
memoria_simulada = [
    "TokenUsuario=ABC12345",
    "TokenUsuario=XYZ78900",
    "TokenAdmin=SUPERSECRET",  # Sensible
    "TokenSesion=TEMP56789",
    "ClaveInterna=INTERNALKEY123"
]

# Solicitud malformada enviada por un atacante
def solicitud_malformada(posicion_lectura, cantidad_lineas):
    print(f"\nAtacante solicita lectura desde posición {posicion_lectura} por {cantidad_lineas} líneas:")

    # Lectura fuera de límites (sin validación adecuada)
    try:
        for i in range(posicion_lectura, posicion_lectura + cantidad_lineas):
            print(f"Exfiltrado: {memoria_simulada[i]}")
    except IndexError:
        print("Error: El atacante intentó leer fuera de los límites de la memoria... pero el sistema no lo detuvo.")

# Simulación de ataques
# Un atacante que sabe dónde buscar puede extraer información crítica
solicitud_malformada(2, 2)  # Exfiltra "TokenAdmin"
solicitud_malformada(0, 5)  # Exfiltra toda la memoria
solicitud_malformada(3, 10) # Lectura exagerada que excede la memoria
```

Consejos esenciales

Se recomienda finalizar todas las sesiones activas tras la actualización.

```bash
kill icaconnection -all
kill pcoipConnection -all
```

Esto asegura la invalidez de los tokens previamente expuestos.

Versiones afectadas

- NetScaler ADC y Gateway **14.1** versiones anteriores a **14.1-43.56**
- NetScaler ADC/Gateway **13.1** anteriores a **13.1-58.32**
- NetScaler ADC **13.1-FIPS** y **NDcPP** anteriores a **13.1-37.235-FIPS/NDcPP**
- NetScaler ADC **12.1-FIPS** antes de **12.1-55.328-FIPS**

Actualizaciones correspondientes

- NetScaler ADC y NetScaler Gateway 14.1-43.56 y versiones posteriores
- NetScaler ADC y NetScaler Gateway 13.1-58.32 y versiones posteriores de 13.1
- NetScaler ADC 13.1-FIPS y 13.1-NDcPP 13.1-37.235 y versiones posteriores de 13.1-FIPS y 13.1-NDcPP
- NetScaler ADC 12.1-FIPS 12.1-55.328 y versiones posteriores de 12.1-FIPS

RECOMENDACIONES

- **Audita tu infraestructura**: identifica todas las instancias NetScaler ADC/Gateway y verifica versiones.
- **Aplica las actualizaciones** lo antes posible.
- **Ejecuta los comandos para finalizar sesiones activas** post-upgrade.
- **Revisa cualquier configuración personalizada** antes de actualizar.

NOTICIA COMPLETA

https://devel.group/blog/nuevas-fallas-en-netscaler-permiten-robo-de-tokens-y-control-remoto/

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