Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDADES ALTAS Y CRÍTICAS EN CITRIX ADC Y CITRIX GATEWAY (CVE-2023-3519, CVE-2023-3466, CVE-2023-3467)

19/Julio/2023

CONTENIDO

INTRODUCCIÓN

Citrix ADC y Citrix Gateway, ampliamente utilizados para soluciones seguras de entrega de aplicaciones y acceso remoto, se han encontrado con vulnerabilidades críticas. Estas vulnerabilidades representan riesgos significativos, incluyendo escalada de privilegios y ejecución remota de código.

VULNERABILIDADES ALTAS Y CRÍTICAS EN CITRIX ADC Y CITRIX GATEWAY (CVE-2023-3519, CVE-2023-3466, CVE-2023-3467)

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

ID de alerta:	DSOC-CERT_2023_07_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/07/2023
Es día cero (0 day):	Si

RESUMEN

VULNERABILIDADES DESCUBIERTAS: DESDE XSS HASTA RCE (EJECUCIÓN REMOTA DE CÓDIGO):

- CVE-2023-3466: Reflected Cross-Site Scripting (XSS):
  - Descripción: Esta vulnerabilidad requiere que la víctima acceda a un enlace controlado por el atacante en el navegador mientras se encuentra en una red con conectividad al NSIP. Permite Reflect Cross-Site Scripting, que puede conducir a la ejecución no autorizada de scripts maliciosos.
  - Según el proveedor, la explotación de la vulnerabilidad requiere un conocimiento técnico de bajo nivel y tiene un alto impacto en la confidencialidad, disponibilidad e integridad en los sistemas específicos.
  - Severidad: Calificación 8.3 (Alto)

- CVE-2023-3467: Privilege Escalation to root administrator (nsroot)
    - Descripción: El acceso autenticado a NSIP o SNIP con acceso a la interfaz de administración puede provocar la escalada de privilegios al nivel de administrador raíz (nsroot). Esta vulnerabilidad permite a un atacante con privilegios limitados obtener un control administrativo total.
    - Aunque la explotación de la vulnerabilidad requiere un acceso de bajo nivel al sistema objetivo, el proveedor sugiere que el impacto del problema de la confidencialidad es muy alto.
    - Severidad: Calificación 8 (Alto)

- CVE-2023-3519: Unauthenticated Remote Code Execution
    - Descripción: Esta vulnerabilidad crítica permite a los atacantes remotos no autenticados ejecutar código arbitrario en el dispositivo afectado. Se puede explotar cuando el dispositivo está configurado como puerta de enlace (servidor virtual VPN, proxy ICA, CVPN, proxy RDP) o servidor virtual AAA.
    - Esta es la vulnerabilidad más grave en el anuncio del proveedor. Mientras que un atacante puede acceder al sistema objetivo a través de una conexión de red; No necesita ningún privilegio ni interacción del usuario.
    - Severidad: Calificación 9.8 (Crítica)

Las siguientes versiones compatibles de NetScaler ADC y NetScaler Gateway están afectadas por las vulnerabilidades:

- NetScaler ADC y NetScaler Gateway 13.1 antes de 13.1-49.13
- NetScaler ADC y NetScaler Gateway 13.0 antes de 13.0-91.13
- NetScaler ADC 13.1-FIPS antes de 13.1-37.159
- NetScaler ADC 12.1-FIPS antes de 12.1-55.297
- NetScaler ADC 12.1-NDcPP antes de 12.1-55.297

Nota: NetScaler ADC y NetScaler Gateway versión 12.1 ahora están al final del ciclo de vida (EOL) y son vulnerables.

RECOMENDACIONES

En primer lugar, actualice Citrix ADC y Citrix Gateway a las versiones más recientes que solucionan estas vulnerabilidades:

- NetScaler ADC y NetScaler Gateway 13.1-49.13 y versiones posteriores
- NetScaler ADC y NetScaler Gateway 13.0-91.13 y versiones posteriores de 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 y versiones posteriores de 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.297 y versiones posteriores de 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.297 y versiones posteriores de 12.1-NDcPP

Nota: NetScaler ADC y NetScaler Gateway versión 12.1 ahora está al final del ciclo de vida (EOL). Se recomienda a los clientes que actualicen sus dispositivos a una de las versiones compatibles que solucionan las vulnerabilidades.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidades-altas-y-criticas-en-citrix-adc-y-citrix-gateway-cve-2023-3519-cve-2023-3466-cve-2023-3467/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente