Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Citrix insta a los administradores a parchear el ADC crítico y la omisión de autenticación de Gateway.

08/Noviembre/2022

Contenido

Introducción 3

Vulnerabilidades en Citrix 4

Resumen 4

Recomendaciones 6

Noticia Completa 6

Contactos de soporte 7

INTRODUCCIÓN

Bajo configuraciones específicas, las tres vulnerabilidades pueden permitir que los atacantes obtengan acceso no autorizado al dispositivo, realicen la toma de control de escritorio remoto o eludan la protección de fuerza bruta de inicio de sesión.

VULNERABILIDADES EN CITRIX

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

ID de alerta:	DSOC-CERT_2022_11_08_1
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/08/2022
Es día cero (0 day):	No

RESUMEN

"Tenga en cuenta que solo los dispositivos que funcionan como puerta de enlace (dispositivos que utilizan la funcionalidad SSL VPN o se implementan como un proxy ICA con autenticación habilitada) se ven afectados por el primer problema, que se clasifica como una vulnerabilidad de gravedad crítica", explica el boletín de seguridad de Citrix. .

Citrix Gateway es un servicio SSL VPN que brinda acceso remoto seguro con capacidades de administración de acceso e identidad, ampliamente implementado en la nube o en servidores corporativos locales.

Citrix ADC es una solución de equilibrio de carga para aplicaciones en la nube implementadas en la empresa, lo que garantiza una disponibilidad ininterrumpida y un rendimiento óptimo.

Ambos productos son ampliamente utilizados por organizaciones de todo el mundo, y las tres fallas afectan a las versiones actuales y anteriores que el proveedor respalda activamente.

Las tres vulnerabilidades que afectan tanto a Citrix Gateway como a Citrix ADC son las siguientes:

CVE-2022-27510 : Omisión de autenticación de gravedad crítica mediante una ruta o canal alternativo, explotable solo si el dispositivo está configurado como VPN (Puerta de enlace).

CVE-2022-27513 : Verificación insuficiente de la autenticidad de los datos, lo que permite la toma de control de escritorio remoto a través de phishing. La falla es explotable solo si el dispositivo está configurado como VPN (Puerta de enlace) y la funcionalidad de proxy RDP está configurada.

CVE-2022-27516 : falla del mecanismo de protección de fuerza bruta de inicio de sesión que permite su omisión. Esta vulnerabilidad solo puede explotarse si el dispositivo está configurado como VPN (Gateway) o servidor virtual AAA con la configuración "Max Login Attempts".

"Se recomienda a los clientes afectados de Citrix ADC y Citrix Gateway que instalen las versiones actualizadas relevantes de Citrix ADC o Citrix Gateway lo antes posible", advierte Citrix.

Los defectos anteriores afectan a las siguientes versiones del producto:

Citrix ADC y Citrix Gateway 13.1 antes de 13.1-33.47
Citrix ADC y Citrix Gateway 13.0 anteriores a 13.0-88.12
Citrix ADC y Citrix Gateway 12.1 antes de 12.1.65.21
Citrix ADC 12.1-FIPS antes de 12.1-55.289
Citrix ADC 12.1-NDcPP anterior a 12.1-55.289

Los usuarios de estas versiones de productos que administran dispositivos Citrix por sí mismos deben actualizarse a la última versión disponible lo antes posible.

Los clientes que confían en Citrix para los servicios de administración basados en la nube no necesitan realizar ninguna acción, ya que el proveedor ya aplicó las actualizaciones de seguridad.

Tenga en cuenta que la información sobre las versiones de productos anteriores a la 12.1 que han llegado al final de su vida útil no está disponible, por lo que se recomienda a los clientes que aún usan estas versiones que actualicen a una versión compatible.

Se recomienda a los clientes afectados de Citrix ADC y Citrix Gateway que instalen las versiones actualizadas relevantes de Citrix ADC o Citrix Gateway lo antes posible:

Citrix ADC y Citrix Gateway 13.1-33.47 y versiones posteriores
Citrix ADC y Citrix Gateway 13.0-88.12 y versiones posteriores de 13.0
Citrix ADC y Citrix Gateway 12.1-65.21 y versiones posteriores de 12.1
Citrix ADC 12.1-FIPS 12.1-55.289 y versiones posteriores de 12.1-FIPS
Citrix ADC 12.1-NDcPP 12.1-55.289 y versiones posteriores de 12.1-NDcPP

Tenga en cuenta que las versiones de Citrix ADC y Citrix Gateway anteriores a la 12.1 son EOL y se recomienda a los clientes de esas versiones que actualicen a una de las versiones compatibles.

Puede gestionar las descargas desde este enlace: https://www.citrix.com/downloads/

Recomendaciones

- Planificar una ventana de mantenimiento para aplicar las actualizaciones necesarias.

- Antes de actualizar, realizar un respaldo de las configuraciones y almacenarlo en un sitio seguro.

- Realizar una revisión a las cuentas de usuario para las VPN, las que no estén siendo utilizadas se recomienda deshabilitarlas.

Noticia Completa

https://devel.group/blog/romcom-se-distribuye-mediante-aplicaciones-popularmente-conocidas/

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