USTIC-AV 19/22. Vulnerabilidades críticas en Citrix Gateway y Citrix ADC (09/11/2022)

La **Unidad de Seguridad TIC** de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** de la **publicación** de **tres vulnerabilidades críticas** de omisión de autenticación en **Citrix Gateway y Citrix ADC** que **podrían permitir** a un atacante remoto **obtener acceso no autorizado al dispositivo**, realizar la **toma de control de escritorio remoto o eludir la protección de fuerza bruta de inicio de sesión**.

Detalle

Citrix Gateway es un servicio SSL VPN que brinda acceso remoto seguro con capacidades de administración de acceso e identidad, ampliamente implementado en servidores corporativos locales o en la nube. Citrix ADC es una solución de balanceador de carga para aplicaciones en la nube implementadas en las organizaciones.

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 vulnerabilidad es explotable sólo si el dispositivo está configurado como VPN (puerta de enlace) y la funcionalidad de proxy RDP está configurada.
- **CVE-2022-27516**: Fallo en el mecanismo de protección de fuerza bruta de inicio de sesión que permite omitirlo. Esta vulnerabilidad solo puede explotarse si el dispositivo está configurado como VPN (Gateway) o servidor virtual AAA con la configuración "*Max Login Attempts*".

Debido a la criticidad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a las vulnerabilidades.

Recursos Afectados

- Citrix ADC y Citrix Gateway 13.1, versiones anteriores a 13.1-33.47
- Citrix ADC y Citrix Gateway 13.0, versiones anteriores a 13.0-88.12
- Citrix ADC y Citrix Gateway 12.1, versiones anteriores a 12.1.65.21
- Citrix ADC 12.1-FIPS, versiones anteriores a 12.1-55.289
- Citrix ADC 12.1-NDcPP, versiones anteriores a 12.1-55.289

Recomendaciones Actualizadas (09/11/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

- **Actualizar** inmediatamente a la última versión disponible en cada caso:
  - 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

**Las versiones de Citrix ADC y Citrix Gateway anteriores a la 12.1 han llegado al final de su vida útil, por lo que se recomienda que actualicen a una de las versiones compatibles.*

Referencias

- Citrix Gateway and Citrix ADC Security Bulletin for CVE-2022-27510 CVE-2022-27513 and CVE-2022-27516

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a ayudadigital.sspa@juntadeandalucia.es in dicando en el *Asunto: [Compromiso Citrix0911]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud