Basque CyberSecurity Centre

Citrix Gateway y Citrix ADC (CVE-2022-27510, CVE-2022-27513, CVE-2022-27516)

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Citrix ha publicado un boletín de seguridad donde se reporta que han descubierto vulnerabilidades en Citrix Gateway y Citrix ADC con los identificadores CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516, siendo la primera de ellas de severidad crítica con un CVSS de 9.8.

2. Recursos afectados

- Citrix ADC y Citrix Gateway 13.1 anterior a la versión 13.1-33.47
- Citrix ADC y Citrix Gateway 13.0 anterior a la versión 13.0-88.12
- Citrix ADC y Citrix Gateway 12.1 anterior a la version 12.1.65.21
- Citrix ADC 12.1-FIPS anterior a la version 12.1-55.289
- Citrix ADC 12.1-NDcPP anterior a la versión 12.1-55.289

3. Análisis técnico

Los detalles de las vulenrabilidades tratadas en esta actualización son los siguientes:

CVE-2022-27510: vulnerabilidad de acceso no autorizado a las capacidades de usuario de Gateway.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.8

CWE-288: Derivación de autenticación mediante una ruta o canal alternativo

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-27513: vulnerabilidad de toma de control de escritorio remoto a través de phishing

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.3

CWE-345: Verificación insuficiente de la autenticidad de los datos

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-27516: vulnerabilidad que afecta a la funcionalidad de protección de fuerza bruta de inicio de sesión del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 5.3

CWE-693: Fallo del mecanismo de protección

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Baja
- **Disponibilidad:** Ninguna

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Desde Citrix se recomienda a los clientes afectados de Citrix ADC y Citrix Gateway que instalen las versiones actualizadas de Citrix ADC o Citrix Gateway lo antes posible, siendo las versiones afectadas:

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

Adicionalmente, y sin relación con los CVE citados, se han añadido mejoras de seguridad para ayudar a proteger a los clientes de ataques de contrabando de solicitudes HTTP en las versiones anteriores de Citrix ADC y Citrix Gateway. Los clientes pueden habilitar estas mejoras mediante la interfaz de administración de Citrix ADC que se puede consultar en https://support.citrix.com/article/CTX472830/citrix-adc-http-request-smuggling-reference-guide

5. Referencias Adicionales

- Boletín de seguridad de Citrix
- CVE-2022-27510
- CWE-288
- CVE-2022-27513
- CWE-345
- CVE-2022-27516
- CWE-693
- https://support.citrix.com/article/CTX472830/citrix-adc-http-request-smuggling-reference-guide

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA