Basque CyberSecurity Centre

Vulnerabilidades en Citrix Hypervisor (CVE-2022-3643, CVE-2022-42328, CVE-2022-42329)

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 una actualización de seguridad que resuelve 3 fallos en Citrix Hypervisor 8.2 LTSR CU1, con los identificadores CVE-2022-3643, CVE-2022-42328, CVE-2022-42329, siendo la primera calificada con una severidad crítica y un CVSS de 10.0. Todos ellos pueden permitir que un usuario privilegiado en una máquina virtual invitada haga que el host deje de responder o se bloquee.

2. Recursos afectados

- Citrix Hypervisor 8.2 LTSR CU1

3. Análisis técnico

La vulnerabilidad identificada como CVE-2022-3643 se corresponde con un fallo que produce que los usuarios guest pueden activar el reinicio/aborto/bloqueo de la interfaz NIC a través de netback. Es posible que un usuario guest active un reinicio/aborto/bloqueo de la interfaz NIC en un backend de red basado en Linux mediante el envío de ciertos tipos de paquetes. Se ha informado que esto ocurre con Cisco (enic) y Broadcom NetXtrem II BCM5780 (bnx2x), aunque también puede ser un problema con otras NIC/controladores. En caso de que la interfaz envíe solicitudes con encabezados divididos, netback reenviará aquellas que violen la suposición mencionada anteriormente al núcleo de la red, lo que dará como resultado dicho mal comportamiento.

La métrica de la vulnerabilidad se corresponde de:

CVSS Base: 10.0, crítica

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

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

En cuanto a la vulnerabilidad CVE-2022-42328 se trata de un fallo que permite que los usuarios guest pueden desencadenar interbloqueos en el controlador netback de Linux.

La métrica de la vulnerabilidad se corresponde de:

CVSS Base: 5.3, media

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

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

Por último CVE-2022-42329 es un fallo, que al igual que el anterior, permite que los usuarios guest pueden desencadenar interbloqueos en el controlador netback de Linux.

La métrica de la vulnerabilidad se corresponde de:

CVSS Base: 5.5, media

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

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

4. Mitigación / Solución

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

Por ello, Citrix ha proporcionado una revisión para solucionar estos problemas. Desde Citrix se recomienda que los clientes afectados instalen esta revisión según lo permita su programa de aplicación de actualizaciones. La revisión se puede descargar desde el siguiente enlace:

Citrix Hypervisor 8.2 LTSR CU1: CTX476080

5. Referencias Adicionales

- CVE-2022-3643
- CVE-2022-42328
- CVE-2022-42329
- Actualización de seguridad de Citrix
- Citrix Hypervisor 8.2 LTSR CU1
- Hotfix Citrix Hypervisor 8.2 LTSR CU1: CTX476080

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA