Vulnerabilidad en Citrix uberAgent

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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.

1. Resumen ejecutivo

Citrix ha publicado un aviso de seguridad para tratar **1 vulnerabilidad** de **severidad alta** cuyo identificador es CVE-2024-3902, que afecta al producto Citrix uberAgent. Su explotación puede dar lugar a una condición de escalada de privilegios con impacto en la **confidencialidad** e **integridad** de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera el fallo destacado. Por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- Citrix uberAgent versiones anteriores a la 7.1.2.

  Adicionalmente, las precondiciones que se tienen que dar para la explotación de este error son:

  Para todas las versiones de Citrix uberAgent anteriores a la 7.1.2:

  Al menos una entrada configurada [CitrixADC_Config] más una de las siguientes métricas configuradas:

  [Timer]

  - CitrixADCPerformance
  - CitrixADCvServer
  - CitrixADCGateways
  - CitrixADCInventory

  Además, para las versiones 7.0, 7.0.1, 7.0.2, 7.1, 7.1.1 y 7.1.1 de Citrix uberAgent:

  WmiProvider establecido en PowerShell y al menos una métrica de CitrixSession configurada:

  [Miscellaneous]

  - WmiProvider = PowerShell

  [Timer]

  - CitrixSessionVirtualChannelDetail
  - CitrixSessionConfig

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en este aviso son los siguientes:

CVE-2024-3902: vulnerabilidad de gestión inadecuada de privilegios que conduce a condiciones de escalada de privilegios en el componente uberAgent, debido a que el producto no asigna, modifica, rastrea ni verifica adecuadamente los privilegios de un actor, lo que crea una esfera de control no deseada para el mismo.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 269: Improper Privilege Management

CVSS Base: **7.3**

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

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

4. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En el caso de la vulnerabilidad CVE-2024-3902, Citrix recomienda a los clientes afectados instalen lo antes posible las versiones actualizadas pertinentes de Citrix uberAgent, que son las que se comprenden desde Citrix uberAgent 7.1.2 y las posteriores a esta.

Las últimas versiones de Citrix uberAgent se pueden consultar en el siguiente enlace.

Como medidas de mitigación complementaria desde Citrix se recomienda para todas las versiones de Citrix uberAgent anteriores a la 7.1.2:

Deshabilitar todas las métricas de CitrixADC eliminando las siguientes propiedades del temporizador:

[Timer]

- CitrixADCPerformance
- CitrixADCvServer
- CitrixADCGateways
- CitrixADCInventory

Eliminar todas las entradas [CitrixADC_Config].

Además, para las versiones 7.0, 7.0.1, 7.0.2, 7.1, 7.1.1 y 7.1.1 de Citrix uberAgent

- Asegurarse que WmiProvider esté establecido en WMIC o no esté configurado.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-3902.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY