USTIC-AV 20/22. Vulnerabilidades críticas en Citrix Gateway y productos VMware (15/12/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, del Centro Criptológico Nacional, **avisa** de la publicación de **diversas vulnerabilidades críticas** que **afectan**, por un lado, **a** Citrix ADC y dispositivos **Citrix Gateway y,** por otro**, a productos VMware** que **deben ser atendidas con especial prontitud.**

Vulnerabilidad crítica en Citrix ADC y dispositivos Citrix Gateway

---

Detalle

Citrix ha reportado una vulnerabilidad 0day de severidad crítica, cuya explotación **podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario en los dispositivos vulnerables.** Se ha asignado el identificador **CVE -2022-27518** para esta vulnerabilidad.

El fabricante ha proporcionado los siguientes comandos para determinar si los sistemas son vulnerables o no. Este aspecto radica en determinar si los sistemas Citrix ADC y Gateway han sido configurados como *SAML SP* o SAML IdP:

- `add authentication samlAction`
- `add authentication samlIdPProfile`

Recursos Afectados

- Citrix ADC 12.0 versiones anteriores a 12.1-65.25
- Citrix Gateway 13.0 versiones anteriores a 13.0-58.32
- Citrix Gateway 12.0 versiones anteriores a 12.1-65.25
- Citrix ADC 12.1-FIPS versiones anteriores a 12.1-55.291
- Citrix ADC 12.1-NDcPP versiones anteriores a 12.1-55.291

Mitigación

1º. Solución a las vulnerabilidades:

- **Actualizar** inmediatamente a la última versión disponible en cada caso:
  - **Citrix ADC** y **Citrix Gateway:** **A** la versión Citrix ADC 13.1 y Citrix Gateway 13.1.
  - **Citrix ADC 12.0** y **Citrix Gateway 12.0:** A la versión **12.1.65.25**.
  - **Citrix ADC FIPS** y **Citrix ADC NDcPP**: A a la versión **12.1-55.291** o posteriores.

Vulnerabilidades críticas en productos VMware

Detalle

Se han identificado 9 vulnerabilidades en varios productos de VMware: 2 de severidad crítica, 3 altas y 4 medias. Destacamos principalmente **dos vulnerabilidades críticas**, que se describen a continuación:

- **CVE-2022-31702** (*CVSSv3: 9.8)*: La vulnerabilidad **permite a un atacante remoto ejecutar comandos de shell arbitrarios en el sistema de destino y** existe debido a una validación de entrada inadecuada en la API REST de vRealize Network Insight (vRNI).

  Recursos afectados

  - vRealize Network Insight vRNI

  Para mayor conocimiento, se recomienda revisar el siguiente aviso publicado por el fabricante: VMSA-2022-0031 (vmware.com)

- **CVE-2022-31705**: Un atacante con privilegios administrativos en local podría explotar esta vulnerabilidad y ejecutar código en el *host*. CVSSv3: 9.3.

  Recursos afectados

  - VMware ESXi
  - VMware Workstation Pro / Player (Workstation)
  - VMware Fusion Pro / Fusion (Fusion)
  - VMware Cloud Foundation

  Se recomienda revisar este otro aviso de seguridad del fabricante para ampliar información: VMSA-2022-0033 (vmware.com)

Para el resto de vulnerabilidades, se pueden consultar los identifcadores CVE en los avisos del fabricante VMSA-2022-0030 (vmware.com) y VMSA-2022-0032 (vmware.com)

Mitigación

1º. Solución a las vulnerabilidades:

- **Instalar las actualizaciones indicadas** en la columna *Fixed Version* **o, en caso de no estar disponibles**, **aplicar** las medidas descritas en la columna ***Workarounds*** de las tablas *Response Matrix* descritas en cada aviso.

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.

Referencias

- **Citrix ADC y dispositivos Citrix Gateway**
  - Citrix ADC and Citrix Gateway Security Bulletin for CVE-2022-27518
  - https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12198-ccn-cert-av-18-22-actualizacion-de-seguridad-critica-para-productos-citrix.html
- **VMware**
  - Avisos del fabricante:
    - VMSA-2022-0030
    - VMSA-2022-0031
    - VMSA-2022-0032
    - VMSA-2022-0033

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a ayudadigital.sspa@juntadeandalucia.es indicando en el *Asunto* lo siguiente:

Para Citrix: [Compromiso Citrix1512]

Para VMware: [Compromiso VMware1512]

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