# BOLETÍN DE ALERTA

**Boletín Nro.:** 2020-21

**Fecha de publicación:** 09/07/2020

**Tema:** Múltiples vulnerabilidades de riesgo crítico afectan a productos de Citrix

**Productos afectados:**

- Citrix ADC y Citrix Gateway, anteriores a 13.0-58.30;
- Citrix ADC y NetScaler Gateway, anteriores a 12.1-57.18;
- Citrix ADC y NetScaler Gateway, anteriores a 12.0-63.21;
- Citrix ADC y NetScaler Gateway, anteriores a 11.1-64.14;
- NetScaler ADC y NetScaler Gateway, anteriores a 10.5-70.18;
- Citrix SD-WAN WANOP, anteriores a 11.1.1ay;
- Citrix SD-WAN WANOP, anteriores a 11.0.3d;
- Citrix SD-WAN WANOP, anteriores a 10.2.7 y
- Citrix Gateway Plug-in para Linux, anteriores a 1.0.0.137.

**Descripción:**

Recientemente un grupo de investigadores de seguridad ha descubierto **11 vulnerabilidades**, las cuales han sido catalogadas como **críticas**. A continuación, se detallan brevemente estos fallos con sus respectivos identificadores:

Se identificaron vulnerabilidades de **divulgación de información**. El **CVE-2019-18177**, que afecta a los productos **Citrix ADC** y **Citrix Gateway**, con **SSL VPN** habilitado. Un atacante local autenticado en la **VPN (Virtual Private Network)** podría explotar exitosamente este fallo y acceder a **información confidencial** y/o útil para llevar a cabo otros tipos de ataques. Mientras que, los **CVE-2020-8195** y

CVE-2020-8196, afectan a los productos **Citrix ADC**, **Citrix Gateway** y **Citrix SDWAN WAN-OP**. Un atacante remoto y autenticado en el **NSIP** (dirección IP en la que se accede al dispositivo Citrix con fines de administración) podría explotar exitosamente estos fallos y acceder a **información** útil para realizar otros ataques**.**

Por otro lado, fueron identificadas vulnerabilidades de **escalamiento de privilegios** que permitirían a usuarios autenticados previamente en el sistema elevar sus privilegios. El CVE-2020-8190, afecta a los productos **Citrix ADC** y **Citrix Gateway**, un atacante local con privilegios de **usuario nobody** (el usuario con menor privilegios en el sistema, presente en algunas distribuciones Unix y Linux), podría explotar la vulnerabilidad. Mientras que el CVE-2020-8197, afecta a los productos **Citrix ADC** y **Citrix Gateway** , para explotar la vulnerabilidad el atacante remoto debe estar autenticado en **NSIP.** La vulnerabilidad relacionada con el CVE-2020-8199 afecta al **Plug-in Citrix Gateway para Linux** en donde el atacante local debe tener acceso al sistema Linux con el plug-in instalado.

También fueron reveladas vulnerabilidades de **XSS (Cross-site Scripting)**. El CVE-2020-8191, afecta a los productos **Citrix ADC**, **Citrix Gateway** y **Citrix SDWAN WAN-OP** un atacante remoto no autenticado podría explotar exitosamente esta vulnerabilidad engañando a una víctima con conectividad al **NSIP** para que ingrese a un enlace malicioso desde el navegador y seguidamente inyectar **código JavaScript**. Con respecto al CVE-2020-8198**,** afecta a los productos **Citrix ADC**, **Citrix Gateway**, **Citrix SDWAN WAN-OP.** Para la explotación exitosa es necesario que la víctima inicie sesión como **administrador (nsroot)** en el **NSIP,** de ser así este fallo permitiría a un atacante remoto no autenticado inyectar **código JavaScript** en el contexto del usuario.

El CVE-2020-8187, afecta a los productos **Citrix ADC** y **Citrix Gateway solo en las versiones 12.0 y 11.1**; con **SSL VPN** o **AAA endpoint** habilitado. La explotación

exitosa de este fallo permitiría a un atacante remoto no autenticado generar un ataque de **denegación de servicio (DoS).**

El **CVE-2020-8193**, trata de una vulnerabilidad de **Authorization Bypass** que afecta a los productos **Citrix ADC**, **Citrix Gateway** y **Citrix SDWAN WAN-OP**. Un atacante remoto con acceso a la **NSIP** podría explotar exitosamente esta vulnerabilidad y **escalar privilegios**.

Finalmente, el **CVE-2020-8194** que afecta a los productos **Citrix ADC**, **Citrix Gateway** y **Citrix SDWAN WAN-OP**. Un atacante remoto podría convencer a la víctima para que descargue y ejecute un **binario malicioso** desde la **NSIP** y de tener éxito inyectar **código malicioso** en el dispositivo.

**Impacto:**

La explotación exitosa de estas vulnerabilidades podrían permitir a un atacante inyectar código malicioso, escalar privilegios, obtener acceso a información confidencial, realizar ataques de denegación de servicio (DoS) y en algunos casos, se podría también llegar a comprometer el dispositivo afectado.

**Solución y prevención:**

- Actualizar **Citrix ADC**, **Citrix Gateway** **y** **Citrix SD-WAN WAN-OP**, a las siguientes versiones:
    - Citrix ADC y Citrix Gateway a 13.0-58.30 y versiones posteriores.
    - Citrix ADC y NetScaler Gateway a 12.1-57.18 y versiones posteriores.
    - Citrix ADC y NetScaler Gateway a 12.0-63.21 y versiones posteriores.
    - Citrix ADC y NetScaler Gateway a 11.1-64.14 y versiones posteriores.
    - NetScaler ADC y NetScaler Gateway a 10.5-70.18 y versiones posteriores.
    - Citrix SD-WAN WANOP a 11.1.1a y versiones posteriores.
    - Citrix SD-WAN WANOP a 11.0.3d y versiones posteriores.

- Citrix SD-WAN WANOP a 10.2.7 y versiones posteriores.
- Citrix Gateway Plug-in for Linux a 1.0.0.137 y versiones posteriores.

- En caso de no ser posible la actualización, como medida de mitigación alternativa, Citrix recomienda seguir los consejos disponibles en su documentación oficial para reducir el riesgo de explotación de estas vulnerabilidades.

**Información adicional:**

- https://support.citrix.com/article/CTX276688
- https://www.citrix.com/blogs/2020/07/07/citrix-provides-context-on-security-bulletin-ctx276688/
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-citrix