Citrix lanzó ayer nuevos parches de seguridad para 11 fallas graves que afectan a sus productos de red Citrix Application Delivery Controller (ADC), Gateway y SD-WAN y WAN Optimization Edition (WANOP).

La explotación exitosa de las vulnerabilidades podría permitir a los hackers no autenticados realizar inyecciones de código, revelar información e incluso, realizar ataques de denegación de servicio contra la puerta de enlace o los servidores virtuales de autenticación.

Citrix confirmó que los problemas mencionados no afectan a otros servidores virtuales, como el equilibrio de carga y el cambio de contenido de servidores virtuales.

Entre los dispositivos Citrix SD-WAN y WANOP afectados, se incluyen los modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

La compañía también dijo que las vulnerabilidades no estaban conectadas a una falla de NetScaler de día cero, previamente corregida (CVE-2019-19781), que permitía a los atacantes realizar ejecución de código arbitrario sin autenticación adecuada.

También mencionó que no hay evidencia de que los defectos recientemente revelados sean explotados en la naturaleza y que las barreras para la explotación de estos defectos sean altas.

> *«De las 11 vulnerabilidades, hay seis posibles rutas de ataque, cinco de ellas tienen barreras para la explotación. Dos de los tres posibles ataques restantes requieren adicionalmente alguna forma de acceso existente. Eso significa efectivamente que un actor malicioso externo primero necesitaría obtener acceso no autorizado a un dispositivo vulnerable para poder realizar un ataque»,* dijo el CISO Fermin Serna.

Aunque Citrix no quiso publicar detalles técnicos de las vulnerabilidades, debido a los esfuerzos de los actores maliciosos para aprovechar los parches y la información para realizar ingeniería inversa, los ataques a la interfaz de administración de los productos

podrían resultar en un compromiso del sistema por parte de un usuario no autenticado, o por medio de Cross-Site Scripting (XSS) en la interfaz de administración.

Un adversario también podría crear un enlace de descarga para un dispositivo vulnerable, lo que podría comprometer una computadora local al ser ejecutada por un usuario no autenticado en la red de administración.

Una segunda clase de ataques se refiere a IP virtuales (VIP), que permite a los atacantes montar DoS contra la puerta de enlace o escanear remotamente los puertos de la red interna.

> *«Los atacantes solo pueden discernir si una conexión TLS es posible con el puerto y no pueden comunicarse más con los dispositivos finales»*, dijo Citrix.

Además, una vulnerabilidad separada en Citrix Gateway Plug-in para Linux (CVE-2020-8199), puede otorgar privilegios elevados a un usuario local conectado de un sistema Linux.