Citrix está advirtiendo a los usuarios sobre una grave vulnerabilidad de seguridad en NetScaler Application Delivery Controller (ADC) y Gateway que, según informan, está siendo activamente explotada en la naturaleza.

Identificada como CVE-2023-3519 (puntuación CVSS: 9.8), el problema está relacionado con un caso de inyección de código que podría permitir la ejecución remota de código sin autenticación. Afecta a las siguientes versiones:

- NetScaler ADC y NetScaler Gateway 13.1 antes de 13.1-49.13
- NetScaler ADC y NetScaler Gateway 13.0 antes de 13.0-91.13
- NetScaler ADC y NetScaler Gateway versión 12.1 (actualmente en estado de fin de vida)
- NetScaler ADC 13.1-FIPS antes de 13.1-37.159
- NetScaler ADC 12.1-FIPS antes de 12.1-55.297, y
- NetScaler ADC 12.1-NDcPP antes de 12.1-55.297

La compañía no proporcionó más detalles sobre la vulnerabilidad asociada con CVE-2023-3519, excepto para indicar que se han observado ataques para la vulnerabilidad en *«dispositivos sin mitigación»*. Sin embargo, para que la explotación sea exitosa, se requiere que el dispositivo esté configurado como un Gateway (servidor virtual VPN, ICA Proxy, CVPN, RDP Proxy) o un servidor virtual de autorización y contabilidad (AAA).

Además de CVE-2023-3519, también se han abordado otros dos errores:

- CVE-2023-3466 (puntuación CVSS: 8.3) – Una vulnerabilidad de validación de entrada incorrecta que resulta en un ataque de scripting entre sitios (XSS) reflejado.
- CVE-2023-3467 (puntuación CVSS: 8.0) – Una vulnerabilidad de gestión incorrecta de privilegios que resulta en una escalada de privilegios al administrador raíz (nsroot).

Wouter Rijkbost y Jorren Geurts de Resillion han sido acreditados por informar sobre los

errores. Se han lanzado parches para abordar los tres problemas en las siguientes versiones:

- NetScaler ADC y NetScaler Gateway 13.1-49.13 y versiones posteriores.
- NetScaler ADC y NetScaler Gateway 13.0-91.13 y versiones posteriores de 13.0.
- NetScaler ADC 13.1-FIPS 13.1-37.159 y versiones posteriores de 13.1-FIPS.
- NetScaler ADC 12.1-FIPS 12.1-55.297 y versiones posteriores de 12.1-FIPS.
- NetScaler ADC 12.1-NDcPP 12.1-55.297 y versiones posteriores de 12.1-NDcPP.

Se recomienda a los clientes de NetScaler ADC y NetScaler Gateway versión 12.1 que actualicen sus dispositivos a una versión compatible para mitigar posibles amenazas.

Estos acontecimientos se producen en medio de la explotación activa de fallos de seguridad descubiertos en Adobe ColdFusion (CVE-2023-29298 y CVE-2023-38203) y en el plugin WooCommerce Payments de WordPress (CVE-2023-28121).

Dejar vulnerabilidades de seguridad sin corregir en los plugins de WordPress podría dar paso a un compromiso completo, permitiendo que actores maliciosos redirijan los sitios de WordPress comprometidos para llevar a cabo otras actividades maliciosas.

El mes pasado, eSentire hizo pública una campaña de ataque llamada Nitrogen, en la que los sitios de WordPress infectados se usaron para alojar archivos ISO maliciosos que, al ejecutarse, desplegaban archivos DLL falsos capaces de contactar con un servidor remoto para obtener más carga maliciosa, incluyendo scripts de Python y Cobalt Strike.

CVE-2023-3519 añadido al catálogo KEV de CISA

La Agencia de Ciberseguridad e Infraestructura (CISA) de EE. UU. incluyó el miércoles la vulnerabilidad de ejecución remota de código de Citrix en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en evidencias de explotación activa. Por este motivo, se exige que las agencias del Poder Ejecutivo Civil Federal (FCEB) solucionen el problema antes del 9 de agosto de 2023 para asegurar sus redes contra posibles amenazas.