BOLETÍN DE ALERTA

Boletín Nro.: 2024-04
Fecha de publicación: 18/01/2024
Tema: Vulnerabilidades críticas en Netscaler ADC (Citrix ADC) y Netscaler Gateway (Citrix Gateway)

Productos afectados:

- NetScaler ADC y NetScaler Gateway 14.1 hasta 14.1-12.35
- NetScaler ADC y NetScaler Gateway 13.1 hasta 13.1-51.15
- NetScaler ADC y NetScaler Gateway 13.0 hasta 13.0-92.21
- NetScaler ADC 13.1-FIPS hasta 13.1-37.176
- NetScaler ADC 12.1-FIPS hasta 12.1-55.302
- NetScaler ADC 12.1-NDcPP hasta 12.1-55.302

Descripción:

Se han reportado vulnerabilidades tipo zero-day identificadas como CVE-2023-6548 y CVE-2023-6549, que afectan a la interfaz de administración de Netscaler ADC, exponiendo instancias no parcheadas a ataques de Ejecución Remota de Código (RCE) y Denegación de Servicio (DoS).
Para lograr la ejecución de código (RCE), es necesario que el actor malicioso haya iniciado sesión en cuentas con mínimos privilegios en el sistema afectado, accediendo a la interfaz de gestión.
Por otra para explotar la vulnerabilidad de denegación de servicio (DoS) el sistema afectado debe estar configurados como gateway (Servidor VPN, ICA Proxy, CVPN, RDP Proxy) o un servidor virtual AAA para ser vulnerables a los ataques de Denegación de Servicio (DoS).

Impacto:

Un actor malicioso podría realizar ataques de ejecución remota de código (RCE) y denegación de servicio (DoS) en los sistemas afectados por la vulnerabilidad.

Recomendación:

Se recomienda a los administradores a parchear los dispositivos afectados de inmediato, bloquear el tráfico de red a las instancias afectadas si no se pueden aplicar las actualizaciones de seguridad de inmediato, y separar el tráfico hacia la interfaz de gestión del tráfico normal.

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-atlassian-0
- https://www.bleepingcomputer.com/news/security/atlassian-warns-of-critical-rce-flaw-in-older-confluence-versions/

- https://nvd.nist.gov/vuln/detail/CVE-2023-22527
- https://nvd.nist.gov/vuln/detail/CVE-2023-22526/change-record?changeRecordedOn=01/16/2024T00:15:07.933-0500
- https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html