

## ALERTA DE SEGURIDAD DE LA INFORMACIÓN “CITRIX BLEED”: VULNERABILIDAD CRÍTICA EN CITRIX NETSCALER EXPLOIT PÚBLICAMENTE DISPONIBLE TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) del Ministerio del Interior y Seguridad Pública comparte con la comunidad información adicional sobre una vulnerabilidad crítica que afecta a NetScaler ADC y NetScaler Gateway de Citrix, identificada como CVE-2023-4966 y conocida como “Citrix Bleed”, de la que informamos en el siguiente enlace: <https://csirt.gob.cl/vulnerabilidades/9vsa23-00915-01/>.

CVE-2023-4966 permite realizar la revelación de información sensible y puede ser explotada de forma remota, lo que le hizo merecedora de un puntaje CVSS de 9.4. Si bien el parche se dio a conocer el 10 de octubre, Mandiant estima que “Citrix Bleed” ha sido explotada desde agosto de este año para robar sesiones de autenticación y tomando el control de cuentas, evadiendo los requerimientos de autenticación, incluyendo la autenticación multifactorial. Un PoC exploit fue publicado esta semana.

**En vista de lo anterior, reforzamos la necesidad de actualizar cuanto antes estos programas con tal de implementar los parches de seguridad respectivos.** Esto incluye, por supuesto, después de la instalación terminar todas las sesiones activas y persistentes, entre otras medidas que se incluyen en la siguiente guía de remediación: <https://services.google.com/fh/files/misc/citrix-netscaler-adc-gateway-cve-2023-4966-remediation.pdf>

Versiones vulnerables:

- NetScaler ADC y NetScaler Gateway 14.1 anteriores a 14.1-8.50
- NetScaler ADC y NetScaler Gateway 13.1 anteriores a 13.1-49.15
- NetScaler ADC y NetScaler Gateway 13.0 anteriores a 13.0-92.19
- NetScaler ADC 13.1-FIPS anteriores a 13.1-37.164
- NetScaler ADC 12.1-FIPS anteriores a 12.1-55.300
- NetScaler ADC 12.1-NDcPP anteriores a 12.1-55.300
- NetScaler ADC y NetScaler Gateway versión 12.1 están en End-of-Life (EOL) y también son vulnerables.

Recuerden que siempre pueden escribir al CSIRT de Gobierno al correo electrónico [incidentes@interior.gob.cl](mailto:incidentes@interior.gob.cl), o llamar al 1510.

Fuentes y más información:

- Boletín de seguridad de Citrix: <https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967>
- Remediation for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966): <https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966>

### CONTACTO Y REDES SOCIALES CSIRT

# Alerta de Seguridad de la Información





Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT  
Coordinación Nacional de Ciberseguridad  
Ministerio del Interior y Seguridad Pública  
Gobierno de Chile



COMUNICADO 10CND23-00116-01 | 26 de octubre de 2023 |

- Citrix NetScaler ADC/Gateway: CVE-2023-4966 Remediation:  
<https://services.google.com/fh/files/misc/citrix-netscaler-adc-gateway-cve-2023-4966-remediation.pdf>
- Citrix Bleed: Leaking Session Tokens with CVE-2023-4966:  
<https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966>

## CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>