| | |
|---|---|
| Alerta de seguridad informática | 9VSA20-00108-02 |
| Numeración anterior | 9VSA-000108-001* |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de Enero de 2020 |
| Última revisión | 21 de Enero de 2020 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

*Este informe tenía

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Citrix, referente a una vulnerabilidad que afecta sus productos Citrix ADC, Citrix Gateway y Citrix SD-WAN WANOP, los cuales de ser explotados, permitirían a un atacante realizar la ejecución de código remoto sobre el sistema afectado. Este informe incluye la respectiva mitigación.

## Vulnerabilidades

CVE-2019-19781

## Impacto

Esta vulnerabilidad permitiría a un atacante remoto sin autenticación realizar ataques de ejecución de remoto arbitrario debido a un error en el balanceador de carga y aprovechándose de una vulnerabilidad de tipo directorio transversal. Es de urgencia aplicar las mitigaciones publicadas por Citrix, pues esta vulnerabilidad ya tiene exploits conocidos, compromete de manera grave al sistema afectado y no es difícil de ejecutar.

## Productos Afectados

Citrix ADC y Citrix Gateway versión 13.0 (todas las builds con soporte).
Netscaler ADC y Netscaler Gateway versión 12.1 (todas las builds con soporte).
Netscaler ADC y Netscaler Gateway versión 12.0 (todas las builds con soporte anteriores a la 12.0.63.13).
Netscaler ADC y Netscaler Gateway versión 11.1 (todas las builds con soporte anteriores a la 11.1.63.15).
Netscaler ADC y Netscaler Gateway versión 10.5 (todas las builds con soporte).
Software y dispositivos Citrix SD-WAN WANOP modelos 4000, 4100, 5000 y 5100 (todas las builds con soporte).

## Mitigación

Para subsanar esta vulnerabilidad, Citrix urge a todos sus clientes a aplicar las mitigaciones publicadas, siendo éstas las mismas para los 3 productos.

https://support.citrix.com/article/CTX267679

Se recomienda utilizar la siguiente herramienta para verificar que se ha mitigado correctamente la vulnerabilidad.

https://support.citrix.com/article/CTX269180

Fechas actualizaciones de seguridad:

Para las versiones 10.5, 12.1 y 13.0 de Citrix ADC y Citrix Gateway, se publicará la actualización el 24 de enero.

Para las versiones 10.2.6 y 11.0.3 de Citrix SD-WAN WANOP, se publicará la actualización el 24 de enero.

Para la versión 11.0 de Citrix ADC y Citrix Gateway, aplicar la build 11.1.63.15.

Para la versión 12.0 de Citrix ADC y Citrix Gateway, aplicar la build 12.0.63.13.

https://www.citrix.com/downloads/citrix-adc/
https://www.citrix.com/downloads/citrix-gateway/

Enlaces

https://support.citrix.com/article/CTX267027

https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-19781

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.21 14:54:09 -03'00'