Alerta de seguridad informática	9VSA-00108-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de diciembre de 2019
Última revisión	24 de diciembre de 2019

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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Citrix referente a una vulnerabilidad crítica que afecta a sus productos, la cual, de ser explotada, permitiría a un atacante remoto acceder a la red local de la víctima. El documento también incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-19781

Impactos

La explotación de esta vulnerabilidad no requiere que el atacante esté de forma local, ni autenticado. Cualquier atacante externo podría acceder a las aplicaciones publicadas y otros recursos en la red interna desde los servidores Citrix. Dependiendo de la configuración de los servidores, las aplicaciones Citrix se pueden usar para conectarse a estaciones de trabajo y sistemas comerciales críticos. Teniendo en cuenta que las aplicaciones de Citrix son accesibles en el perímetro de la red de la empresa, la vulnerabilidad podría permitir a los atacantes acceder a otros recursos en la red interna desde el servidor Citrix.

Producto Afectado

Citrix ADC y Citrix Gateway versión 13.0 (todas las compilaciones soportadas).
Citrix ADC y Netscaler Gateway versión 12.1 (todas las compilaciones soportadas).
Citrix ADC y Netscaler Gateway versión 12.0 (todas las compilaciones soportadas).
Citrix ADC y Netscaler Gateway versión 11.1 (todas las compilaciones soportadas).
Citrix Netscaler ADC y Netscaler Gateway versión 10.5 (todas las compilaciones soportadas).

Mitigación

Se deben aplicar los siguientes pasos publicados en la URL a continuación para mitigar la vulnerabilidad hasta que Citrix publique un parche para solucionarla:
https://support.citrix.com/article/CTX267679

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: 2019.12.24 10:39:44 -03'00'