Alerta de seguridad cibernética	9VSA20-00263-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de julio de 2020
Última revisión	08 de julio 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Citrix respecto a 11 vulnerabilidades que afectan a sus productos Citrix ADC, Citrix Gateway y Citrix SD-WAN edición WANOP. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2019-18177
CVE-2020-8187
CVE-2020-8190
CVE-2020-8191
CVE-2020-8193
CVE-2020-8194
CVE-2020-8195
CVE-2020-8196
CVE-2020-8197
CVE-2020-8198
CVE-2020-8199

Además, para evitar confusión, Citrix ha dispuesto de 5 puntos que podrían aclarar ciertos temas:

- Los últimos parches resuelven todas las vulnerabilidades.
- De las 11 vulnerabilidades, existen 6 vectores de ataque; 5 de ellos requieren de traspasar ciertas barreras para su explotación.
- As it relates to CTX276688, here are five important points to understand:
- No se conocen exploits para ninguna de las vulnerabilidades.
- El producto Citrix-managed Gateway no es afectado por las vulnerabilidades.
- Ninguna de las vulnerabilidades tiene relación con el CVE-2019-19781. https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00108-02/

CVE-2019-18177

Vulnerabilidad de tipo filtración de información, requiere que el atacante esté autenticado vía VPN y una configuración SSL en el endpoint VPN.

Productos Afectados
Citrix ADC y Citrix Gateway.

CVE-2020-8187

Vulnerabilidad de tipo denegación de servicios, requiere una configuración SSL en el endpoint VPN o AAA, y el atacante no necesita estar autenticado.

Productos Afectados
Citrix ADC y Citrix Gateway versiones 12.0 y 11.1.

CVE-2020-8190

Vulnerabilidad de tipo escalación de privilegios de forma local, requiere que el atacante esté autenticado en el NSIP y que ya haya obtenido privilegios “nobody” utilizando otro ataque.

Productos Afectados
Citrix ADC y Citrix Gateway.

CVE-2020-8191

Vulnerabilidad de tipo XSS reflejado (Cross-site Scripting), requiere que la víctima se encuentre en la red, con conectividad al NSIP, y que abra un enlace diseñado especialmente, enviado por el atacante, para realizar el ataque.

Productos Afectados
Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8193

Vulnerabilidad de tipo evasión de autorización, requiere que el atacante tenga acceso al NSIP pero no es necesario que se encuentre autenticado.

Productos Afectados

Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8194

Vulnerabilidad de tipo inyección de código, requiere que la víctima descargue y ejecute un binario malicioso desde el NSIP.

Productos Afectados

Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8195

Vulnerabilidad de tipo filtración de información, requiere que el atacante esté autenticado en el NSIP.

Productos Afectados

Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8196

Vulnerabilidad de tipo filtración de información, requiere que el atacante esté autenticado en el NSIP.

Productos Afectados

Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8197

Vulnerabilidad de tipo elevación de privilegios, requiere que el atacante esté autenticado en el NSIP.

Productos Afectados
Citrix ADC y Citrix Gateway.

CVE-2020-8198

Vulnerabilidad de tipo XSS almacenado (Cross-site Scripting), requiere que la víctima esté con privilegios de administrador (nsroot) en el NSIP.

Productos Afectados
Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.

CVE-2020-8199

Vulnerabilidad de tipo elevación de privilegios local, requiere que el atacante esté de forma local en el computador que esté ejecutado el Plug-in.

Productos Afectados
Citrix Gateway Plug-in para Linux.

MITIGACIONES

Para subsanar las vulnerabilidades, actualizar a las versiones mencionadas a continuación:
Citrix ADC y Citrix Gateway 13.0-58.30 y lanzamientos posteriores.
Citrix ADC y NetScaler Gateway 12.1-57.18 y lanzamientos posteriores.
Citrix ADC y NetScaler Gateway 12.0-63.21 y lanzamientos posteriores.
Citrix ADC y NetScaler Gateway 11.1-64.14 y lanzamientos posteriores.
NetScaler ADC y NetScaler Gateway 10.5-70.18 y lanzamientos posteriores.
Citrix SD-WAN WANOP 11.1.1a y lanzamientos posteriores.
Citrix SD-WAN WANOP 11.0.3d y lanzamientos posteriores.
Citrix SD-WAN WANOP 10.2.7 y lanzamientos posteriores.
Citrix Gateway Plug-in para Linux 1.0.0.137 y versiones posteriores

Enlaces

https://github.com/squid-cache/squid/security/advisories/GHSA-w7pw-2m4p-58hr
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8187
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8191
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8195
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8196
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8197
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8198
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8199