

Alerta de seguridad informática	9VSA-00092-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de noviembre de 2019
Última revisión	30 de noviembre 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 del sitio oficial de Mozilla, referente a una vulnerabilidad que afecta a servicios de seguridad de red, la cual, si es explotada, puede resultar en ejecución de código remoto. Adjunto en este informe se publican los enlaces para descargar las respectivas actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-11745

Impacto

Por falta de sanitización en la función NSC_EncryptUpdate(), alojada en /lib/softoken/pkcs11c.c, un atacante podría comprometer al sistema pasando datos especialmente diseñados a la aplicación afectada para generar un desbordamiento del búfer en memoria y así poder ejecutar código remoto. La complejidad de la ejecución de este ataque es alta, pero también lo es el impacto a la confidencialidad, integridad y disponibilidad.

Producto Afectado

Las siguientes versiones de Mozilla NSS son vulnerables:

3.0.1	3.24
3.1 y 3.1.1	3.25 y 3.25.1
3.2 hasta 3.2.2	3.26 hasta 3.26.2
3.3 hasta 3.3.11	3.27 hasta 3.27.2
3.4 hasta 3.4.5	3.28 hasta 3.28.6
3.5	3.29 hasta 3.29.5
3.6 y 3.6.1	3.30 hasta 3.30.2
3.7 hasta 3.7.11	3.31 y 3.31.1
3.8 hasta 3.8.2	3.32 y 3.32.1
3.9 hasta 3.9.5	3.33
3.10 hasta 3.10.2	3.34 y 3.34.1
3.11 hasta 3.11.10	3.35
3.12 hasta 3.12.11	3.36 hasta 3.36.8
3.13 hasta 3.13.6	3.37 hasta 3.37.3
3.14 hasta 3.14.5	3.38
3.15 hasta 3.15.5	3.39
3.16 hasta 3.16.6	3.40 y 3.40.1
3.17 hasta 3.17.4	3.41 y 3.41.1
3.18 y 3.18.1	3.42 y 3.42.1
3.19 hasta 3.19.4	3.43
3.20 hasta 3.20.2	3.44 hasta 3.44.2
3.21 hasta 3.21.4	3.45
3.22 hasta 3.22.3	3.46 y 3.46.1
3.23	3.47

Mitigación

Actualizar a la versión 3.44.3 o 3.47.1, más información en el siguiente URL:

<https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>

Enlaces

- <https://hg.mozilla.org/projects/nss/rev/4c20de402b3901df0cde590a46be2ba49adc028e>
- <https://hg.mozilla.org/projects/nss/rev/60bca7c6dc6dc44579b9b3e0fb62ca3b82d92eec>
- <https://www.cybersecurity-help.cz/vdb/SB2019112801>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11745>