Alerta de Seguridad Informática

Alerta de seguridad informática	9VSA-00042-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de septiembre de 2019
Última revisión	02 de septiembre 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 la información entregada por DEBIAN referente vulnerabilidades detectadas en varios productos del servicio Apache2 httpd y sus respectivas actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-9517

Impacto

Algunas implementaciones HTTP/2 son vulnerables a almacenamiento interno de datos en buffer sin restricciones. El atacante podría realizar un ataque de denegación de servicio inundando una conexión con solicitudes, lo cual puede producir un exceso de consumo en CPU, memoria, o ambas.

Productos Afectados

- Release: stretch – Versión: 2.4.25-3+deb9u7
- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: stretch (security) – Versión: 2.4.25-3+deb9u8
- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://nvd.nist.gov/vuln/detail/CVE-2019-9517

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9517
https://security-tracker.debian.org/tracker/CVE-2019-9517

Vulnerabilidad

CVE-2019-10081

Impacto

Usando HTTP/2 (desde 2.4.20 hasta 2.4.39) con ‘’pushes’’ al comienzo, por ejemplo configurado con “HWPushResource”, se puede provocar una sobre escritura de memoria en el grupo de solicitudes de inserción, lo que provoca caídas y bloqueos. La memoria copiada es la configurada en los valores push del encabezado del enlace, no la ingresada por el cliente.

Productos Afectados

- Release: stretch – Versión: 2.4.25-3+deb9u7
- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: stretch (security) – Versión: 2.4.25-3+deb9u8
- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10081
https://nvd.nist.gov/vuln/detail/CVE-2019-10081
https://security-tracker.debian.org/tracker/CVE-2019-10081

Vulnerabilidad

CVE-2019-10082

Impacto

Manejo de la sesión HTTP/2 podría permitir la lectura de memoria anteriormente liberada en el cierre de la conexión.

Productos Afectados

- Release: stretch – Versión: 2.4.25-3+deb9u7
- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: stretch (security) – Versión: 2.4.25-3+deb9u8
- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://security-tracker.debian.org/tracker/CVE-2019-10082

Vulnerabilidad

CVE-2019-10092

Impacto

El atacante podría provocar un error en el enlace de la página de error “mod_proxy”, y modificarlo para apuntar a otra página, así logrando engañar a los usuarios. Esta vulnerabilidad requiere que durante la configuración del servidor con proxy, se cometan errores, para que la página de error pueda renderizarse.

Productos Afectados

- Release: jessie – Versión: 2.4.10-10+deb8u12
- Release: stretch – Versión: 2.4.25-3+deb9u7
- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: jessie (security) – Versión: 2.4.10-10+deb8u15
- Release: stretch (security) – Versión: 2.4.25-3+deb9u8
- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://security-tracker.debian.org/tracker/CVE-2019-10092

Vulnerabilidad

CVE-2019-10097

Impacto

Cuando mod_remoteip se configura para usar un servidor proxy intermediario confiable usando el protocolo “PROXY”, un encabezado PROXY manipulado podría desencadenar un desbordamiento del buffer basado en pila o una desferencia de puntero NULO. Esto solo puede ser activado por un proxy confiable y no por clientes HTTP no confiables.

Productos Afectados

- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://security-tracker.debian.org/tracker/CVE-2019-10097

Vulnerabilidad

CVE-2019-10098

Impacto

Los redireccionamientos configurados con mod_rewrite, que debían ser autorreferenciales, podrían ser engañados por nuevas líneas de código y en su lugar redirigir a una URL diferente dentro de la URL de solicitud.

Productos Afectados

- Release: jessie – Versión: 2.4.10-10+deb8u12
- Release: stretch – Versión: 2.4.25-3+deb9u7
- Release: buster – Versión: 2.4.38-3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Release: stretch (security) – Versión: 2.4.25-3+deb9u8
- Release: buster (security) – Versión: 2.4.38-3+deb10u1

Enlace

https://security-tracker.debian.org/tracker/CVE-2019-10098
https://unaaldia.hispasec.com/2019/08/actualizacion-de-seguridad-de-apache2-para-debian.html