Agosto 2018

Nº BS201808001

Importancia: ALTA

Riesgo Explotacion: ALTA

Vulnerabilidad grave en Kernel de Linux

Las versiones del kernel de Linux 4.9+ y las versiones compatibles de FreeBSD son vulnerables a las condiciones de denegación de servicio con bajas tasas de paquetes especialmente modificados.

Las versiones de kernel de Linux 4.9+ pueden verse forzadas a realizar llamadas repetitivas a tcp_collapse_ofo_queue () y tcp_prune_ofo_queue () para cada paquete entrante que puede conducir a una denegación de servicio.

Productos afectados:

https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=962459&SearchOrder=4

Link alertas:

CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion') - CVE-2018-5390

CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion') - CVE-2018-6922

Recomendaciones:

- Los parches para el kernel de Linux están disponibles para abordar la vulnerabilidad.
- Parches para FreeBSD están disponibles para abordar la vulnerabilidad.
- Aún existen fabricantes que están evaluando la vulnerabilidad y podrían hasta la fecha de publicación del presente boletín no haber publicado el parche respectivo.

Referencias:

- https://git.kernel.org/pub/scm/linux/kernel/git/davem/net.git/commit/?id=1a4f14bab1868b443f0dd3c55b689a478f82e72e
- https://www.spinics.net/lists/netdev/msg514742.html
- https://www.freebsd.org/security/advisories/FreeBSD-SA-18:08.tcp.asc

Este boletín de seguridad es producido por el Cert Nacional el Perú (PeCERT), el mismo incluye información sensible que puede impactar en su organización, si tiene alguna duda o necesita mayor información no dude en contactarse con nosotros a través del correo pecert@pcm.gob.pe o nuestra central telefónica +51 219-7000 Anexo 5111, 5129