BOLETIN DE ALERTA

El día de ayer, lunes 07/04/2014 ha sido reportada una vulnerabilidad en OpenSSL, versión 1.0.1f/1.0.2-beta1 e inferiores. La vulnerabilidad ha sido clasificada como extremadamente crítica. La función `dtls1_process_heartbeat/dtls1_process_heartbeat` en la biblioteca *ssl/t1_lib.c* del componente *TLS/DTLS Heartbeat Handler* es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase information disclosure (exposición de información sensible). Esto tiene repercusión sobre la confidencialidad.

Un exploit ha sido desarrollado por Jared Stafford en Python y publicado. El exploit puede ser descargado de http://downloads.securityfocus.com/vulnerabilities/exploits/66690.py

En el siguiente link puede comprobar si su servidor es vulnerable:
http://rehmann.co/projects/heartbeat/

Para eliminar la vulnerabilidad recomendamos urgentemente actualizar a la versión 1.0.1g disponible en:
https://www.openssl.org/source/
Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de:
http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902
El mejor modo sugerido para mitigar el problema es actualizar a la última versión.

Información adicional:
http://heartbleed.com/
https://www.openssl.org/news/secadv_20140407.txt

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Complejo Santos E2 - Gral. Santos 1170 c/ Concordia
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py