REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	METROBANK S.A
Fecha	5/07/2018
Servicio	MSS-VME
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones detectó que TLS versión 1.0 está habilitado en los siguientes hosts:190.34.183.148,190.34.183.91,190.34.183.132,190.34.183.149,190.34.183.152,190.34.183.154. La versión 1.0 de TLS, tiene una serie de defectos criptográficos conocidos (en el diseño) que lo hacen vulnerable a cierto tipo de ataques. Las versiones más recientes de TLS, 1.1 y 1.2, están diseñadas contra estos defectos. GLESEC recomienda habilitar la versión TLS 1.2 y, de ser posible y mientras no represente introduzca una falla de disponibilidad en producción, habilitar la recién aprobada TLS versión 1.3.

ACCIONES A TOMAR

Se deben deshabilitar las versiones 1.1 y 1.0 de TLS y permitir conexiones TLS sólo con la versión 1.2 (o 1.3, de ser aplicable).

COMENTARIOS Y RECOMENDACIONES

Recomendamos tomar las acciones de actualizar las versiones de TLS a la versión más reciente. Puede acceder al siguiente link de referencia, donde comunica que la fecha límite de soporte para estas versiones finaliza el 30 de junio de 2018.

Fuente de referencia:

https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTES DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimento con el protocolo de Semáforo (TLP) del Departamento de Seguridad de Estado de Estados Unidos (DHS): TLP -Blanco (Divulgación no limitada), TLP-Verde (Divulgación Limitada, Restringida, solo para la comunidad), TLP-Ámbar (Divulgación Limitada, Restringida, Para los participantes de la Organización) y TLP-Rojo (No Divulgación, Restringida/Confidencial – Solo compartida con el US DHS).

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355