REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	Metrobank, S.A
Fecha	24/10/2018
Servicio	MSS-VME
Nivel de Severidad	Media
Nivel de Impacto	Media
Nivel de Vulnerabilidad	Media

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones ha detectado que existen 3 vulnerabilidades medias en uno de sus sistemas, estas catalogadas como TLS v1.1 habilitado, SSL STATIC KEY CIPHERS (conjuntos de cifrado de clave estática) habilitado y TLS Diffie Hellman modulus menor a 2048, el sistema afectado está asociado a dirección IP externa 190.34.183.131 y nombre de dominio www.govimar.com.pa.

ACCIONES A TOMAR

Configurar el sistema afectado para usar grupos Diffie-Hellman más fuertes con primos seguros de 2048 bits en adelante.

Configure el sistema afectado para deshabilitar la compatibilidad con los conjuntos de cifrado de clave estática. Para los servidores web de Microsoft IIS, consulte el artículo 245030 de Microsoft Knowledgebase para obtener instrucciones sobre cómo deshabilitar los conjuntos de cifrado de clave estática. La siguiente configuración recomendada proporciona un mayor nivel de seguridad. Esta configuración es compatible con Firefox 27, Chrome. 22, IE 11, Opera 14 y Safari 7.

Configure el sistema afectado para que requiera que los clientes utilicen la versión 1.2 de TLS

mediante el cifrado autenticado con datos asociados (AEAD por sus siglas en ingles).

COMENTARIOS Y RECOMENDACIONES

GLESEC recomienda seguir los puntos mencionados en la sección *Acciones a Tomar* para reducir el riesgo en su organización.

El estándar de seguridad de datos PCI (Payment Card Industry) requiere un mínimo de TLS v1.1 y recomienda TLS v1.2. Adicionalmente. El estándar FIPS 140-2 requiere un mínimo de TLS v1.1 y recomienda TLS v1.2. Los protocolos SSLv2, SSLv3 y TLSv1 no se recomiendan en esta configuración.

Las estimaciones actuales son que una el equipo académico puede romper un Prime de 768 bits y un actor a nivel estatal puede romper un Prime de 1024 bits.

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