

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	METROBANK
Fecha	13/11/2018
Servicio	MSS-VM
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones, dando un seguimiento al problema de la aplicación eBanking, hemos investigado y se detectó que el host <https://190.34.183.154>, presenta un error Web al tratar de acceder a las direcciones <https://190.34.183.154/> y <https://metronet.metrobanksa.com/> como se muestra en la siguiente imagen:

Nota: este error fue notificado por ustedes por correo electrónico el jueves 8 de noviembre de 2018.

← → ↻ 🏠 <https://metronet.metrobanksa.com>

SRVE0255E: No se ha definido un host WebGroup/Virtual para manejar /.

SRVE0255E: No se ha definido un host WebGroup/Virtual para manejar metronet.metrobanksa.com:443.

Sin embargo, este error no se presenta al acceder a través del enlace https://metronet.metrobanksa.com/DIBS_METROBANK_BP/pages/loginP.jsp

Adicionalmente, este host posee vulnerabilidades relacionadas a SSL como la detección de SSL v2 y v3, suites de cifrado SSL de seguridad media.

ACCIONES A TOMAR

Verificar los hosts presentados anteriormente, hacer las configuraciones necesarias en la aplicación Web para que este error no se presente y mitigar las vulnerabilidades descubiertas en este host.

COMENTARIOS Y RECOMENDACIONES

Para las vulnerabilidades de SSL, es recomendable actualizar los servicios para que utilicen TLS 1.2 o 1.3. SSL ya no es considerado un protocolo seguro y TLS es considerado el estándar para las comunicaciones seguras hoy día.

CONFIDENTIAL



REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTE DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimiento 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).

CONFIDENTIAL

