REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	METROBANK
Fecha	11/10/2018
Servicio	MSS-VM
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones les brinda un resumen de las vulnerabilidades detectadas en sus sistemas mediante rango de IP otorgada por el cliente. Las vulnerabilidades presentadas son:

- MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check), en el host 190.34.183.131.
- SSL Version 2 and 3 Protocol Detection, en los hosts: 190.34.183.152, 190.34.183.149, 190.34.183.91.
- SSL Certificate Cannot Be Trusted, en los hosts: 190.34.183.132, 190.34.183.91, 190.34.183.90.
- SSL DROWN Attack Vulnerability en el host 190.34.183.149.

ACCIONES A TOMAR

Verificar los hosts presentados anteriormente y mitigar las vulnerabilidades que fueron detectadas en ellos.

COMENTARIOS Y RECOMENDACIONES

La vulnerabilidad HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check) es una actualización de seguridad que se considera crítica para todas las ediciones compatibles de Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1 y Windows Server 2012 R2.
Se recomienda aplicar parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

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).