REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	Metrobank, SA
Fecha	25/05/2018
Servicio	MSS-VM
Nivel de Severidad	Critical
Nivel de Impacto	Critical
Nivel de Vulnerabilidad	Critical

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones encontró una vulnerabilidad Crítica en el host IP 190.34.183.131, esta vulnerabilidad afecta sistemas Windows para servidores versiones: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 y Windows Server 2008 R2 for x64-based Systems Service Pack 1.

Microsoft cataloga esta vulnerabilidad como: “Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)” y fue publicada en “Microsoft Security bulletin MS15-034 – Critical”. CVE-2015-1635.

Esta vulnerabilidad permite la ejecución de código arbitrario en el sistema, el atacante podría utilizar una petición HTTP especialmente creada para explotar esta debilidad y esto le permitiría ejecución de código en el contexto de la cuenta del sistema.

ACCIONES A TOMAR

Aplicar todas las actualizaciones de seguridad sugeridas por Windows, en especial MS15-034 (KB 3042553), ya que todas estas dan solución a vulnerabilidades encontradas en este tipo de sistema y deben mantenerse al día.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

COMENTARIOS Y RECOMENDACIONES

Al aplicar la actualización de seguridad se mitiga esta vulnerabilidad, ya que esta modifica la manera en que el stack HTTP de Windows maneja las peticiones HTTP.

GLESEC recomienda que se mitigue la misma en el menor tiempo posible.

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