REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	31/08/2018
Servicio	MSS-VME
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones detectó que el protocolo SSL versiones 2 y 3 están habilitados en los siguientes hosts:

- 200.90.137.87
- 200.90.137.89
- 200.90.137.83
- 200.46.227.230
- 200.46.19.100

Estas versiones de SSL se ven afectadas por varios defectos criptográficos que lo hacen vulnerable a cierto tipo de ataques:

1. Estos servidores admiten SSL v2, que es OBSOLETO e INSEGURO (por ejemplo, con el ataque **DROWN**).

2. Estos servidores son vulnerables al ataque de **POODLE**. Se recomienda deshabilitar SSL v3 para mitigar.

GLESEC recomienda habilitar el protocolo TLS versión 1.2.

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

COMENTARIOS Y RECOMENDACIONES

Consulte la documentación de la aplicación para deshabilitar SSLv 2.0 y 3.0. Utilice TLS 1.2 con el conjunto de cifrado aprobados.

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