REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	BANVIVIENDA
Fecha	28/05/2018
Servicio	MSS-SIEM
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones ha encontrado que, en el día de hoy y por repetidas veces, la dirección IP pública 200.46.161.233 ha intentado acceder vía TELNET al host con dirección IP 200.46.227.227 correspondiente al dispositivo Cisco ASA de sus instalaciones. La resolución DNS de la IP potencialmente atacante es:

```
Name:    233-161.46.200.alianzaviva.net
Address:  200.46.161.233
```

Estos intentos de conexión han sido denegados, los hemos observado usando el servicio MSS-SIEM contratado por ustedes; sin embargo la insistencia de éstos desde una dirección pública (perteneciente al rango de direcciones asignados a Panamá) es para iniciar una investigación de su parte.

ACCIONES A TOMAR

GLESEC ALERTA que si el servicio TELNET está habilitado en el host con dirección IP 200.46.227.227 (o en cualquier otro host de la organización); DESHABILITARLO INMIEDIATAMENTE (aún si su uso es sólo interno) y sustituirlo por SSH v2.

Recomendamos que, de no ser necesario, no exponer servicios a la red pública (y, en general, al

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

ofrecer servicios, pensar siempre en el mínimo privilegio).

COMENTARIOS Y RECOMENDACIONES

GLESEC recomienda que nunca se utilice TELNET para establecer conexiones hacia sus sistemas, este servicio debe estar deshabilitado ya que es considerado como inseguro.

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).