REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	10/09/2018
Servicio	MSS-SIEM
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro centro de Operaciones encontró excesivas perdidas de sincronización con el host remoto 64.76.57.232; un aproximado de 20 mil eventos cada hora. Esto puede ser el resultado de un error de configuración en cualquiera de los extremos de la conexión asociada a este registro.

<163>1 2018-09-10T10:47:25-05:00 200.46.19.98 %ASA-3-713902 - - - Group = 64.76.57.232, IP = 64.76.57.232, Removing peer from correlator table failed, no match!

<163>1 2018-09-10T10:47:25-05:00 200.46.19.98 %ASA-3-713902 - - - Group = 64.76.57.232, IP = 64.76.57.232, QM FSM error (P2 struct &0xcca403d0, mess id 0x84804d9c)!

ACCIONES A TOMAR

1. Verificar si la conexión VPN al host **64.76.57.232** es permitida.
2. Revisar la configuración de la VPN en el dispositivo asociado a la dirección IP 200.46.19.98; esta debe concordar con la configuración que se tiene para esta conexión en el host remoto 64.76.57.232 de manera tal que pueda funcionar apropiadamente. Verifique la configuración ISAKMP y el mapa criptográfico en ambos pares.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

COMENTARIOS Y RECOMENDACIONES

Este problema puede causar sobrecarga en el dispositivo, ya que de manera regular registra un error que no se soluciona. Si la conexión con este host remoto, en específico, es parte de algún proceso antiguo que ya no se utiliza; se recomienda sacar esta dirección del rango permitido de las conexiones VPN. Podría ser necesario solucionar los problemas de la configuración para determinar la causa del error.

Links oficiales relevantes con respecto a este tema:

- ✓ https://community.cisco.com/t5/vpn-and-anyconnect/asa-5510-l2l-vpn-internal-error/td-p/1368897
- ✓ https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog/syslogs7.html

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