Incidencia de vulnerabilidad

Organizacion	Banvivienda
Fecha	Febrero 23, 2018
Servicio	MSS-VME
Seguridad nivel	Medium
Impacto Nivel	Medium
Vulnerabilidad Nivel	Medium

Descripción

En nuestro sistema de monitoreo (GOC) y usando el servicio MSS-VME contratado por ustedes, detectamos lo siguiente:

1. El servicio de versión 1 de IKE (Internet Key Exchange) parece ser compatible con el modo agresivo con autenticación de clave pre compartida (PSK). Tal configuración podría permitir a un atacante capturar y crackear la PSK de una puerta de enlace VPN y obtener acceso no autorizado a redes privadas.

Sistemas Afectados

Port	Host
500 / udp / ikev1	200.46.19.98, 200.46.227.227, 200.46.227.227

Solución
- Desactiva el modo agresivo si es compatible.
- No use la clave pre compartida para autenticación si es posible.
- Si no se puede evitar el uso del clave pre compartida, use claves muy fuertes.
- Si es posible, no permita conexiones VPN desde ninguna dirección IP.

GLESEC, recomienda aplicar estas recomendaciones a la BREVEDAD posible, a fin de mitigar el riesgo de explotación de estas vulnerabilidades.

Saludos Cordiales y reiterándole siempre nuestra disposición en prestarle un servicio de alta calidad y acorde a sus expectativas, se despide;

GLESEC OPERATION CENTER – GOC.