YOUR GLOBAL CYBER-SECURITY PARTNER

Incidente De Vulnerabilidad

organizacion	Metrobank
Fecha	Noviembre 14, 2017
Servicio	MSS-VME
Seguridad nivel	Medium
Impacto Nivel	Medium
Vulnerabilidad Nivel	Medium

Descripcion

Host name vulnerable: mail.metrobanksa.com (190.34.183.149)

En nuestro sistema de monitoreo (GOC) y usando el servicio MSS-VME contratado por ustedes, detectamos en su servidor las siguientes vulnerabilidades:

1. Este servidor admite SSL 2, que es OBSOLETO e INSEGURO (por ejemplo, con el ataque DROWN). Se recomienda deshabilitarlo.
2. Este servidor es vulnerable al ataque de POODLE. Se recomienda deshabilitar SSL 3 para mitigar.
3. El servidor admite protocolos más antiguos, pero no el TLS 1.2, que es actual y mejor. Se recomienda habilitar TLS 1.2 y colocar como protocolo de preferencia.
4. Este servidor acepta el cifrado RC4 (el cual es ALTAMENTE INSEGURO), se recomienda deshabilitar en el CypherSuite todas las negociaciones que incluyan RC4.

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

Estamos atentos ante cualquier duda o inquietud de su parte.

Saludos Cordiales,

GLESEC OPERATION CENTER – GOC.