## Incidencia de vulnerabilidad

| | |
|---|---|
| **Organizacion** | Banvivienda |
| **Fecha** | Febrero 06, 2018 |
| **Servicio** | MSS-VME |
| **Seguridad nivel** | Medium |
| **Impacto Nivel** | Medium |
| **Vulnerabilidad Nivel** | Medium |

# Description

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

1. Estos servidores admiten SSL 2, que es OBSOLETO e INSEGURO (por ejemplo, con el ataque DROWN). Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.
Utilice TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

Sistemas Afectados

| Port | Host |
|---|---|
| 443 / tcp / www | 200.46.227.230, 200.46.227.230 |

2. Estos servidores son vulnerables al ataque de POODLE. Se recomienda deshabilitar SSL 3 para mitigar.

Sistemas Afectados

| Port | Host |
|---|---|
| 443 / tcp / www | 200.46.19.100, 200.46.19.100, 200.90.137.83, 200.90.137.83 |

3. Los servidores admiten 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. Estos servidores aceptan el cifrado RC4 (el cual es ALTAMENTE INSEGURO), se recomienda deshabilitar en el CypherSuite todas las negociaciones que incluyan RC4.

Sistemas Afectados

| Port | Host |
|---|---|
| 25 / tcp / smtp | 200.90.137.87, 200.90.137.89 |

CONFIDENTIAL

443 / tcp / www  200.90.137.94, 200.90.137.94
443 / tcp / www  200.46.19.100, 200.46.19.100, 200.90.137.83, 200.90.137.83
443 / tcp / www  200.46.227.230 200.46.227.230

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.***

CONFIDENTIAL