Incidencia de seguridad

Organizacion	Banvivienda
Fecha	Noviembre 29, 2017
Servicio	MSS-VME
Seguridad nivel	Medium
Impacto Nivel	Medium
Vulnerabilidad Nivel	Medium

Descripción

Hosts vulnerables: 200.90.137.87 y 200.90.137.89

Recibimos con mucho agrado la noticia que la vulnerabilidad **Heartbleed,** reportada por el Centro de Operaciones de GLESEC (GOC) en noviembre 13 de 2017, fue solucionada por ustedes, según email enviado a nosotros en fecha 24 noviembre.

Haciendo un nuevo análisis bajo pedido de los dos IP mencionados, nuestro servicio de gestión de vulnerabilidades (MSS-VME) detectó nuevas vulnerabilidades relacionadas con los protocolos SSL/TLS (implementados en la aplicación OpenSSL)

En éstas, se consideran inseguros aquellas suites de cifrado que utilicen los algoritmos de cifrado **DES**, **3DES** e **IDEA** y el algoritmo de hash **SHA-1**.

GLESEC, recomienda eliminar de la suite todas las entradas relacionadas con los algoritmos mencionados.

Los detalles de estas vulnerabilidades se muestran a continuación:

Sistemas Afectados: 200.90.137.87 y 200.90.137.89

```
Lista de suites de cifrado de bloques de 64 bits admitidas por el
servidor remoto:

  Cifrados de intensidad media (> 64 bits y <clave de 112 bits, o 3DES)

    EDH-RSA-DES-CBC3-SHA Kx = DH Au = RSA Enc = 3DES-CBC (168) Mac = SHA1
    DES-CBC3-SHA Kx = RSA Au = RSA Enc = 3DES-CBC (168) Mac = SHA1

  Cifrados de alta resolución (> = clave de 112 bits)

    IDEA-CBC-SHA Kx = RSA Au = RSA Enc = IDEA-CBC (128) Mac = SHA1
```

```
Los campos de arriba son:

  {OpenSSL nombre de cifrado}
  Kx = {intercambio de claves}
  Au = {autenticación}
  Enc = {método de cifrado simétrico}
  Mac = {mensaje de código de autenticación}
  {exportar bandera}
```

```
Los siguientes certificados fueron parte de la cadena de certificados
enviados por el host remoto, pero contiene hashes que se consideran
débiles.

| Sujeto: C = US / O = McAfee, Inc./OU=Email
Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
| Algoritmo de firma: SHA-1 con encriptación RSA
| -Válido desde: 10 de octubre 22:51:42 2014 GMT
| -Válido a: 07 de octubre 22:51:42 2024 GMT
```

```
Aquí está la lista de cifradores SSL de intensidad media admitidos por el
servidor remoto:

  Cifrados de intensidad media (> 64 bits y <clave de 112 bits, o 3DES)

    EDH-RSA-DES-CBC3-SHA Kx = DH Au = RSA Enc = 3DES-CBC (168) Mac = SHA1
    DES-CBC3-SHA Kx = RSA Au = RSA Enc = 3DES-CBC (168) Mac = SHA1

Los campos de arriba son:

  {OpenSSL nombre de cifrado}
  Kx = {intercambio de claves}
  Au = {autenticación}
  Enc = {método de cifrado simétrico}
  Mac = {mensaje de código de autenticación}
  {exportar bandera}
```

Por cualquier consulta nos hacen saber.

Cordialmente,

GLESEC OPERATIONS CENTER -GOC