Incidencia de vulnerabilidad

organizacion	Banvivienda
Fecha	Noviembre 13, 2017
Servicio	MSS-VME
Seguridad nivel	Critico
Impacto Nivel	Critico
Vulnerabilidad Nivel	Critico

Descripcion

Hosts vulnerables: 200.90.137.87 200.90.137.89

En nuestro sistema de monitoreo (GOC) y usando el servicio MSS-VME contratado por ustedes, detectamos la vulnerabilidad conocida como **Heartbleed**, la cual permite a un atacante interceptar comunicaciones seguras y robar información confidencial como credenciales de acceso, datos personales, o incluso las claves para descifrar. Rogamos aplicar la solución a la BREVEDAD posible, a fin de mitigar el riesgo de explotación de esta vulnerabilidad.

Detalles de las vulnerabilidades en su sistema:

Divulgación de información de Heartbeat de OpenSSL (Heartbleed)

Descripción

En función de su respuesta a una solicitud de TLS con un mensaje de latido especialmente diseñado (RFC 6520), el servicio remoto parece verse afectado por un error de lectura fuera de límites.

Este error podría permitir a un atacante remoto leer los contenidos de hasta 64 KB de memoria del servidor, lo que podría exponer contraseñas, claves privadas y otros datos confidenciales.

Salidas

Se pudo leer la siguiente memoria desde el servicio remoto:

0x0000: 45 74 4D 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE EtM ..> .....
0x0010: FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7 .....
0x0020: 00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2 .....
0x0030: 00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4 ..... |.} ....

0x0040: 00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6 ..... ~ ....
0x0050: 00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF ..... + ...
0x0060: C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B.,. R ... s .....
0x0070: CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8 ... /. 0.v ... w ....
0x0080: C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32.-... t ... u ... 1.2
0x0090: C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8 .x ... y .....
0x00A0: 00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F .....
0x00B0: CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE .....
0x00C0: C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B ..... z. {
0x00D0: 00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87 .ce .... 2.8.D ..
0x00E0: 00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14 ... f .....
0x00F0: 00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B ... 3.9.E .....
0x0100: 00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E ... 0.6.B .....
0x0110: 00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19 ... 1.7.C .....
0x0120: 00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18 ..... 4.:. F .....
0x0130: 00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13 .....
0x0140: C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02 .....
0x0150: C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18 .....
0x0160: C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28 .....). &. *. '. +. (
0x0170: 00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20. # ... "...%.!. $.
0x0180: 00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60 ..... ba`
0x0190: 00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92 d .....
0x01A0: 00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01 ... /. 5.A .....
0x01B0: 00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3 ..... @. J ....
0x01C0: 00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE ..... -... gk.
0x01D0: 00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC ...>. H .....?. I ..
0x01E0: 00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34 ... lm .... #. $. 4
0x01F0: C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33 .5.7.6.8.9.:.;. 3.....

Systemas Afectados

Ports	Hosts
25 / tcp / smtp	200.90.137.89

Salidas

Se pudo leer la siguiente memoria desde el servicio remoto:

```
0x0000: 69 45 4E 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE iEN ..> ..........
0x0010: FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7 ................
0x0020: 00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2 ................
0x0030: 00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4 ......... |.} ....
0x0040: 00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6 ........... ~ ....
0x0050: 00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF ........... + ....
0x0060: C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B.,. R ... s ........
0x0070: CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8 ... /. 0.v ... w ....
0x0080: C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32.-... t ... u ... 1.2
0x0090: C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8 .x ... y ..........
0x00A0: 00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F ................
0x00B0: CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE ................
0x00C0: C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B ............. z. {
0x00D0: 00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87 .ce .... 2.8.D ..
0x00E0: 00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14 ... f ............
0x00F0: 00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B ... 3.9.E ........
0x0100: 00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E ... 0.6.B ........
0x0110: 00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19 ... 1.7.C ........
0x0120: 00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18 ..... 4.:. F ......
0x0130: 00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13 ................
0x0140: C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02 ................
0x0150: C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18 ................
0x0160: C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28 .....). &. *. '. +. (
0x0170: 00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20. # ... "...%.!. $.
0x0180: 00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60 ........... ba`
0x0190: 00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92 d ..............
0x01A0: 00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01 ... /. 5.A ........
0x01B0: 00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3 ......... @. J ....
0x01C0: 00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE ..... -... gk.
0x01D0: 00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC ...>. H .....?. I ..
0x01E0: 00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34 ... lm .... #. $. 4
0x01F0: C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33 .5.7.6.8.9.:.;. 3
0x0200: C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83. '. (.%. &.). * ....
0x0210: 00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6 ........., ......
0x0220: 00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0 ......... <. = ....
0x0230: 00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A.; ..... "....! ..
```

0x0240: C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00 ... ... O .....
0x0250: 3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00>. <.....
0x0260: 07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00 .....
0x0270: 0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 .....
0x0280: 17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00 .....
0x0290: 0B 00 04 03 00 01 02 12 02 01 02 03 02 02 04 01 .....
0x02A0: 04 03 05 01 05 03 06 01 06 03 00 00 00 00 00 00 .....
0x02B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
*
0x1000:

Systemas Afectados

Ports	Hosts
25 / tcp / smtp	200.90.137.87

Solución
Actualice a OpenSSL 1.0.1g o posterior.

Alternativamente, recompile OpenSSL con el indicador '-DOPENSSL_NO_HEARTBEATS' para deshabilitar la funcionalidad vulnerable.

Exploit disponible: Si
Explotación fácil: los exploits están disponibles

Vulnerabilidad MiTM 'ChangeCipherSpec' de OpenSSL

Descripción
El servicio OpenSSL en el host remoto es vulnerable a un ataque man-in-the-middle (MiTM), basado en la aceptación de un protocolo de enlace especialmente diseñado.

Esta falla podría permitir a un atacante MiTM desencriptar o falsificar mensajes SSL al decirle al servicio que comience las comunicaciones encriptadas antes de que se intercambie el material clave, lo que hace que las claves predecibles se usen para asegurar el tráfico futuro.

Tenga que solo se ha probado una vulnerabilidad SSL / TLS MiTM (CVE-2014-0224). Sin embargo, ha inferido que el servicio OpenSSL en el host remoto también se ve afectado por seis vulnerabilidades adicionales que se revelaron en el aviso de seguridad de OpenSSL del 5 de junio de 2014:

- Existe un error en la función 'ssl3_read_bytes' que permite inyectar datos en otras sesiones o permite ataques de denegación de servicio. Tenga en cuenta que este problema es explotable solo si SSL_MODE_RELEASE_BUFFERS está habilitado. (CVE-2010-5298)

- Existe un error relacionado con la implementación del Algoritmo de Firma Digital de Curva Elíptica (ECDSA) que permite la divulgación de nonce a través del ataque de canal lateral de caché 'FLUSH + RELOAD'. (CVE-2014-0076)

- Existe un error de desbordamiento de búfer relacionado con el manejo de fragmentos de DTLS no válidos que permite la ejecución de código arbitrario o permite ataques de denegación de servicio.
Tenga en cuenta que este problema solo afecta a OpenSSL cuando se usa como cliente o servidor DTLS. (CVE-2014-0195)

- Existe un error en la función 'do_ssl3_write' que permite desreferenciar un puntero NULL, lo que podría permitir ataques de denegación de servicio. Tenga en cuenta que este problema es explotable solo si SSL_MODE_RELEASE_BUFFERS está habilitado. (CVE-2014-0198)

- Existe un error relacionado con el manejo de handshake de DTLS que podría permitir ataques de denegación de servicio. Tenga en cuenta que este problema solo afecta a OpenSSL cuando se usa como cliente DTLS.
(CVE-2014-0221)

- Existe un error en la función 'dtls1_get_message_fragment' relacionado con las suites anónimas de cifrado ECDH. Esto podría permitir ataques de denegación de servicio. Tenga en cuenta que este problema solo afecta a los clientes de OpenSSL TLS. (CVE-2014-3470)

OpenSSL no lanzó parches individuales para estas vulnerabilidades, sino que todos fueron parcheados bajo una sola versión de la versión. Tenga en cuenta que el servicio seguirá siendo vulnerable después del parcheo hasta que se reinicie el servicio o el host.

Salidas:
El servicio remoto en el puerto 25 aceptó un mensaje ChangeCipherSpec anterior, que causó
las claves MAC y de cifrado se derivan por completo de la información pública. Todo el SSL
El apretón de manos se completó, con el servidor aceptando y produciendo mensajes cifrados y autenticado usando estas teclas débiles.

Solución

Los usuarios de OpenSSL 0.9.8 SSL / TLS (cliente y / o servidor) deberían actualizar a 0.9.8za. Los usuarios de OpenSSL 1.0.0 SSL / TLS (cliente y / o servidor) deberían actualizar a 1.0.0m. Los usuarios de OpenSSL 1.0.1 SSL / TLS (cliente y / o servidor) deberían actualizar a 1.0.1h.

Systemas Afectados

Ports	Hosts
25 / tcp / smtp	200.90.137.87 200.90.137.89

Exploit disponible: Si
Explotación fácil: los exploits están disponibles

Por cualquier consulta nos hacen saber.

Sinceramente,

GLESEC OPERATION CENTER – GOC.