



HISPASEC SISTEMAS

SEGURIDAD Y TECNOLOGÍAS
DE LA INFORMACIÓN

**Informe técnico:
Denegación de servicio en Asterisk
Agosto 2009**

Hugo Teso, Hispasec Lab



Índice

1	INTRODUCCIÓN	3
2	DESCRIPCIÓN	3
3	PRUEBA DE CONCEPTO	6
4	SOLUCIÓN	6

Hispacec Sistemas S.L.

Avda Juan López Peñalver, 17
Edificio Centro de Empresas CEPTA
Parque Tecnológico de Andalucía
29590 Campanillas (Málaga)

Telf: (+34) 902 161 025
Fax: (+34) 952 028 694

Información General
info@hispacec.com

Comercial
comercial@hispacec.com

www.hispasec.com

Copyright

El Copyright de este documento es propiedad de Hispasec Sistemas S.L. Hispasec Sistemas S.L. proporciona este documento bajo la condición de que será tratado con confidencialidad. No está permitida su reproducción total o parcial ni su uso con otras organizaciones para ningún otro propósito, excepto autorización previa por escrito.

1 Introducción

Se ha confirmado la existencia de una vulnerabilidad en Asterisk, que podría permitir a un atacante remoto provocar una denegación de servicio en los sistemas vulnerables.

Asterisk es una aplicación de una central telefónica (PBX) de código abierto. Como cualquier PBX, se pueden conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectarlos a un proveedor de VoIP para realizar comunicaciones con el exterior. Asterisk es ampliamente usado e incluye un gran número de interesantes características: buzón de voz, conferencias, IVR, distribución automática de llamadas, etc. Además el software creado por Digium está disponible para plataformas Linux, BSD, MacOS X, Solaris y Microsoft Windows.

2 Descripción

Producto: Asterisk

Resumen: Vulnerabilidad remota de tipo DoS

Severidad: Alta

CVE: CVE-2009-2726

Se han reportado múltiples vulnerabilidades de tipo Denegación de Servicio que afectan al Software de telefonía IP Asterisk; dichas vulnerabilidades tienen su origen en un uso inseguro de la función *sscanf* de la librería estándar de C.

La función *sscanf* es la encargada dentro de la librería estándar de C de leer datos formateados de una cadena. Lee los datos de la cadena y los almacena de acuerdo al formato indicado en las localizaciones especificadas por argumentos adicionales.

```
int sscanf(const char *cadena, const char *formato,...);
```

Esta función se emplea en varios puntos del código de Asterisk para extraer valores numéricos de textos ASCII en mensajes SIP entrantes.

SIP (Protocolo de Inicio de Sesiones) es un protocolo desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el vídeo, voz, mensajería instantánea o juegos online.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en Internet.

Wikipedia

La raíz de fallo radica en el hecho de que las llamadas a *sscanf* normalmente no especifican un tamaño máximo para los campos a extraer con lo que, por defecto, *sscanf* asigna un tamaño máximo infinito.

Un ejemplo de uso inseguro de esta función sería:

```
if (!error && sscanf(cseq, "%d%n", &seqno, &len) != 1) {
```

Si un atacante enviase un mensaje SIP con un gran número de caracteres ASCII decimales en la posición de un campo que vaya a ser extraído por *sscanf* podría llegar a agotar la memoria de la pila produciendo una condición de DoS.

A continuación se muestra un ejemplo de datagrama malicioso que provocaría el DoS:

```
0000 00 0c 29 00 00 00 00 50 56 00 00 00 08 00 45 00  ..).y$.P V.....E.
0010 05 dc c0 c2 20 00 40 11 78 fa c0 a8 4d 02 c0 a8  .... .@. x...M...
0020 4d 01 b7 9e 13 c4 83 0b 07 de 49 4e 56 49 54 45  M..... ..INVITE
0030 20 73 69 70 3a 62 6f 62 40 31 39 32 2e 31 36 38  sip:bob @192.168
0040 2e 37 37 2e 31 20 53 49 50 2f 32 2e 30 0d 0a 56  .77.1 SI P/2.0..V
0050 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44 50 20  ia: SIP/ 2.0/UDP
0060 31 39 32 2e 31 36 38 2e 37 37 2e 32 3a 34 37 30  192.168. 77.2:470
0070 30 36 3b 62 72 61 6e 63 68 3d 7a 39 68 47 34 62  06;branc h=z9hG4b
0080 4b 4e 44 66 34 77 6c 53 73 44 64 3b 72 70 6f 72  KNDf4w1S sDd;rpor
0090 74 0d 0a 54 6f 3a 20 22 42 6f 62 22 20 3c 73 69  t..To: " Bob" <si
00a0 70 3a 62 6f 62 40 31 39 32 2e 31 36 38 2e 37 37  p:bob@19 2.168.77
00b0 2e 31 3e 0d 0a 46 72 6f 6d 3a 20 22 41 6c 69 63  .1>..Fro m: "Alic
00c0 65 22 20 3c 73 69 70 3a 61 6c 69 63 65 40 31 39  e" <sip: alice@19
00d0 32 2e 31 36 38 2e 37 37 2e 32 3e 3b 74 61 67 3d  2.168.77 .2>;tag=
00e0 63 48 43 47 73 38 4e 54 51 69 0d 0a 43 61 6c 6c  cHCGs8NT Qi..Call
00f0 2d 49 44 3a 20 73 69 70 5f 69 6e 76 69 74 65 5f  -ID: sip _invite_
0100 62 79 65 2e 69 6e 76 69 74 65 2e 68 65 61 64 65  bye.invi te.heade
0110 72 73 2e 63 2d 73 65 71 2e 76 61 6c 75 65 2e 73  rs.c-seq .value.s
0120 65 71 2e 70 72 65 70 65 6e 64 3a 30 2b 6e 72 69  eq.prepe nd:0+nri
0130 54 64 6c 7a 37 4d 78 40 6d 75 64 79 6e 61 6d 69  Tdlz7Mx@ mudynami
0140 63 73 2e 63 6f 6d 0d 0a 43 53 65 71 3a 20 30 30  cs.com.. CSeq: 00
0150 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000 00000000
...
05d0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000 00000000
05e0 30 30 30 30 30 30 30 30 30 30 00000000 00
```

A continuación se muestra el mismo datagrama con el contenido desglosado:

```
###[ Ethernet ]###
dst= 00:0c:29:00:00:00
src= 00:50:56:00:00:00
```



```
+                                } else if (sscanf(pri, "%30d", &ipri) != 1 &&
@@ -1639,9 +1639,9 @@
-                                if (sscanf(chan, "%d-%d", &start, &finish) == 2) {
+                                if (sscanf(chan, "%30d-%30d", &start, &finish) == 2) {
                                        /* Range */
-                                } else if (sscanf(chan, "%d", &start)) {
+                                } else if (sscanf(chan, "%30d", &start)) {
```

3 Prueba de concepto

Los paquetes SIP necesarios para probar la efectividad de este fallo se pueden crear con la herramienta Sipsak (SIP swiss army knife), un generador de paquetes al estilo Nemesis o Scapy pero especializado en el protocolo SIP. Se puede encontrar más información sobre esta herramienta en su página web: <http://sipsak.org/>

Para reproducir las condiciones que propician un DoS tan sólo hay que enviar un paquete SIP Invite con alguno de los campos vulnerables (Cseq, Content-Length o SDP) asignado a un valor numérico muy largo (por ejemplo unos 32768 ceros).

4 Solución

Actualizar a la última versión de Asterisk para la rama empleada en las versiones 1.2.34, 1.4.26.1, 1.6.0.12 y 1.6.1.4.

Más Información:

Asterisk Project Security Advisory - AST-2009-005
Remote Crash Vulnerability in SIP channel driver

<http://downloads.asterisk.org/pub/security/AST-2009-005.html>

