UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA- UNAM

Boletín de Seguridad UNAM-CERT 2003-006

Múltiples Vulnerabilidades en Implementaciones de SIP (Session Initiation Protocol).

El **CERT/UNAM-CERT**, a través de sus equipos de respuesta a incidentes de **Seguridad en Cómputo**, han emitido éste boletín en el cual informan que han sido reportadas numerosas vulnerabilidades en múltiples implementaciones de distribuidores de SPI (Session Initiation Protocol).

Estas vulnerabilidades pueden permitir a un intruso obtener accesos a privilegios no autorizados, causar ataques de negación de servicio, o causar un comportamiento inestable en el sistema. Si algún sitio utiliza productos SIP habilitados en cualquier capacidad, el CERT/UNAM-CER recomiendan que se consulte y analice este boletín, además sugiere que se sigan los pasos proporcionados en la sección de **Solución**.

Fecha de Liberación:	**21 de Febrero de 2003**
Ultima Revisión:	**---**
Fuente:	**CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes.**

SISTEMAS AFECTADOS

Los productos habilitados con SIP de una amplia variedad de distribuidores son afectados. Otros sistemas haciendo uso de SIP pueden también ser vulnerables pero no han sido probados específicamente. No todas las implementaciones de SIP son afectadas. Consulte la sección **Información de Distribuidores** para obtener más detalles de los distribuidores que han proporcionado información a este boletín.

Además de los distribuidores que han proporciona información a este boletín, una lista de distribuidores que el CERT/UNAM-CERT han contactado en relación a estos problemas esta disponible en la Nota de Vulnerabilidad VU#528719.

DESCRIPCIÓN

ISP (Session Initiation Protocol) es un protocolo nuevo en desarrollo que es utilizado comúnmente en Voz sobre IP (VoIP), telefonía en Internet, mensajería instantánea y otras varias aplicaciones. SIP es un protocolo basado en texto para iniciar sesiones de comunicación y datos entre usuarios.

El Grupo de Programación Segura de la Universidad de Oulu (OUSPG) ha conducido una investigación previa en las vulnerabilidades en LDAP, culminando en el **Boletín de Seguridad UNAM-CERT 2001-019**, y SMPT, resultando en el **Boletín de Seguridad UNAM-CERT 2002-002**.

La investigación más reciente de OUSPG se ha centrado en un subconjunto de SIP relacionado al mensaje INVITE, el cual es solicitado por agentes SIP y proxy para aceptar una orden de inicio de sesión. Al aplicar conjunto de pruebas PROTOS c07-sip a una variedad de productos habilitados con SIP, OUSPG descubrió impactos que van desde un comportamiento inesperado en el sistema y negación de servicio, hasta la ejecución de código remoto. Se debe hacer notar que "throttling" es un comportamiento inesperado.

Especificaciones para el SIP están disponibles en el RFC3261:

http://www.ietf.org/rfc/rfc3261.txt

OUSPG ha establecido el siguiente sitio que detalla documentación sobre SIP y los resultados de las pruebas de implementación:

http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

La página del IETF Charter para SIP esta disponible en:

http://www.ietf.org/html.charters/sip-charter.html

IMPACTO

La explotación de estas vulnerabilidades puede resultar en condiciones de negación de servicio, interrupción de servicio y en algunos casos puede permitir a un intruso obtener acceso no autorizado al dispositivo afectado. El impacto específico variará de producto a producto.

SOLUCIÓN

Muchos de los pasos de las soluciones recomendados a continuación pueden tener impacto significativo en las operaciones cotidianas de la red y/o en la estructura de la red. Se debe asegurar que los cambios realizados en base a las siguientes recomendaciones no afectarán el desempeño ni la capacidad de conexión a redes externas.

Aplicar una Actualización del Distribuidor.

El **Apéndice A** contiene información de los distribuidores sobre este boletín. Se debe consultar este Apéndice y la Nota de Vulnerabilidad VU#528719 para determinar si algún producto es vulnerable. Si información sobre algún distribuidor no está disponible, consulte directamente a su distribuidor.

Deshabilitar los dispositivos y los servicios con SIP habilitado

Como una regla general, el CERT/UNAM-CERT recomiendan deshabilitar cualquier servicio ó características que no sea explícitamente requeridas. Algunos de los productos afectados probablemente se basan en SIP para ser funcionales. Se debe considerar de forma muy cuidadosa el impacto de bloquear servicios que podrían no estarse utilizando.

Filtrado de Entrada

Como una medida temporal, puede ser posible limitar el alcance de estas vulnerabilidades bloqueando el acceso a los servicios y a los dispositivos SIP en el perímetro de la red.

El filtrado de entrada maneja el flujo de tráfico que entra a la red que esta bajo el control del administrador. Típicamente los servidores son las únicas máquinas que necesitan aceptar tráfico no limitado desde el Internet. La mayoría de los Agentes de Usuario SIP (incluyendo los teléfonos IP o los clientes de software) consisten de un cliente de Agente de Usuario y de un Servidor de Agente de Usuario. En la red se utilizan directivas de muchos sitios, y existen pocas razones para que los servidores externos inicialicen tráfico ilimitado hacia las máquinas que no proporcionan servicios públicos. De esta forma, el filtrado de ingreso debe ser llevado a cabo en la periferia para de esta manera prohibir la inicialización de tráfico externo ilimitado hacia servicios no autorizados. Para SIP, el filtrado de ingreso de los siguientes puertos, puede prevenir que intrusos fuera de la red accedan a dispositivos vulnerables en la red local y que no están explícitamente autorizados a proporcionar servicios públicos de SIP.

```
sip     5060/udp    # Session Initiation Protocol (SIP)
sip     5060/tcp    # Session Initiation Protocol (SIP)
sip     5061/tcp    # Session Initiation Protocol (SIP) over TLS
```

Se debe tener consideraciones cuidadosas para solucionar los tipos de puertos mencionados anteriormente. Los sitios deben planear el filtrado de paquetes como parte de su estrategia para prevenir el exploit de estas vulnerabilidades.

Se debe hacer notar que estas medidas podrían no proteger a los dispositivos vulnerables contra intrusos internos.

Filtrado de Salida

El filtrado de salida maneja el flujo de tráfico que sale de la red que esta bajo

control administrativo. Típicamente existe la necesidad de limitar las máquinas que proporcionan los servicios públicos que inicializan tráfico de salida hacia el Internet. En el caso de las vulnerabilidades en SIP, al emplear el filtrado de salida en los puertos listados anteriormente en el perímetro de la red, puede prevenir que la red sea utilizada como una fuente de ataque contra otros sitios.

Bloquear Requerimientos Dirigidos a Direcciones Broadcast Mediante el Ruteador

Debido a que los requerimientos SIP pueden ser transmitidos vía UDP, los ataques de broadcast son posibles. Una solución para prevenir que el sitio sea utilizado como un intermediario en un ataque es bloquear los requerimientos SIP dirigidos a direcciones broadcast mediante el ruteador

APÉNDICE A. Información Adicional

Este apéndice contiene información proporcionada por los distribuidores de éste boletín. Si un distribuidor en particular reporta nueva información al CERT/UNAM-CERT, esta sección será actualizada.

America Online Inc

No es vulnerable.

Apple Computer Inc.

Actualmente no existen aplicaciones proporcionadas por Apple con MAC OS X ó MAC OS X Server que hagan uso de ISP.

BorderWare

Los productos de BorderWare no hacen uso de SIP, de esta forma, los productos de BorderWare no son afectados por esta vulnerabilidad.

Cisco Systems

Cisco Systems ha direccionando las vulnerabilidades identificadas por #VU528719 a través de toda su línea de productos. Cisco ha liberado un boletín en:

http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml

Clavister

Los productos Clavister actualmente no incorporan soporte para conjunto de protocolo SIP, y por lo tanto, no son vulnerables.

F5 Networks

F5 Networks no tiene un producto servidor SIP, y por lo tanto no es afectado por esta vulnerabilidad.

Fujitsu

Concerniente a VU#528719, el sistema operativo UXP/V de Fujitsu no es vulnerable debido a que la función relevante no es soportada bajo UXP/V.

Hewlett-Packard Company

Fuente:
Hewlett-Packard Company
Software Security Response Team

ID de Referencia: SSRT2402

HP-UX - No es vulnerable
HP-MPE/ix - No es vulnerable
HP Tru64 UNIX - No es vulnerable
HP OpenVMS - No es vulnerable
HP NonStop Servers - No es vulnerable

Para reportar vulnerabilidades de seguridad potenciales en software HP, se debe enviar un correo electrónico a: mailto:security-alert@hp.com

IBM

SIP no es implementado como parte del sistema operativo AIX.

Las vulnerabilidades discutidas en VU#528719 no afectan a AIX.

IP Filter

IP Filter no hace manejo de ningún protocolo SIP en específico y por lo tanto no es afectado por las vulnerabilidades mencionadas en el documento.

IPTel

Todas las versiones de SIP express Router superiores a 0.8.9 son vulnerables al conjunto de pruebas de OUSPG. Se recomienda actualizar a la versión 0.8.10. Se debe aplicar la actualización para la versión 0.8.10 de http://www.iptel.org/ser/security/
antes de la instalación y mantener una observación de este sitio en el futuro.

Juniper Neworks

Los productos de Juniper Networks no usan SIP, y no generan, procesan, o actúan como proxy para mensajes del protocolo SIP. Por lo tanto, los productos de Juniper Networks no son susceptibles a esta vulnerabilidad.

Clientes que deseen utilizar características de filtrado de paquetes de los productos Juniper Networks para bloquear mensajes del protocolo SIP pueden visitar el sitio Web de soporte para los productos Juniper Networks en https://www.juniper.net/support/csc/

o pueden contactar al Centro de Asistencia Técnica de Juniper Networks al teléfono 1-888-314-JTAC (clientes U.S. únicamente; clientes no-U.S. podrán llamar JTAC al +1 408-745-9500.)

Lucent

Los productos Lucent no son afectados por esta vulnerabilidad, sin embargo, se está investigando y se actualizará esta postura si es necesario.

Microsoft Corporation

Microsoft ha investigado sobre estos problemas. La implementación del cliente SIP de Microsoft no es afectada.

NEC Corporation

==========

NEC vendor statement para VU#528719

==========

Liberado el 13 de Febrero, 2002

Productos de Servidor

- Sistema Operativo EWS/UP Serie 48.
- - NO es vulnerable, debido a que no soporta SIP.

Productos de Ruteador

- IX Series 1000 / 2000 / 5000
- - NO es vulnerable, debido a que no soporta SIP.

Otros productos de Red

- Se continúan verificando los productos con soporte para el protocolo SIP.

==========

NetBSD

NetBSD no contiene ninguna implementación de SIP.

NETfilter.org

Debido a que la implementación de linux netfilter 2.4/2.5 actualmente no soporta rastreo de conexión o NAT para el conjunto de protocolo SIP, no es vulnerable a este bug.

NetScreen

NetScreen no es vulnerable a este problema.

Network Appliance

Los productos NetApp no son afectados por esta vulnerabilidad.

Nokia

Plataformas Nokia IP Security basadas en IPSO, plataformas Nokia Small Office Solution, productos VPN de Nokia y la plataforma Nokia Message Protector no inicializan o terminan sesiones basadas en SIP. Los productos Nokia mencionados no son susceptibles a esta vulnerabilidad.

Nortel Networks

Todos los productos que utilizan SIP han sido probados y todos los productos generalmente disponibles, con las siguientes excepciones, han pasado el conjunto de pruebas:

Succession Communication Server 2000 y Succession Communication Server 2000 - Compact son impactados por el conjunto de pruebas son en las configuraciones donde SIP-T ha sido provisionado con el Communication Server; se espera que este disponible una actualización de software a finales de Febrero.

Novell

Novell no tiene productos implementando SIP.

Secure Computing Corporation

Neither Sidewinder no implementa SIP, por lo tanto, no es vulnerable.

SecureWorx

El conjunto de productos SecureWorx Basilisk Gateway Security (Firmware versión 3.4.2 o superior) no son vulnerables a la Vulnerabilidad VU#528719 como se describe en el anuncio de OUSGP (OUSGP#0106) recibido el 8 de Noviembre de 2002.

Stonesoft

El firewall de alta disponibilidad StoneGate de StoneSoft y los productos de VPN no contienen ningún código que maneje el protocolo SIP. Ninguna de las versiones de StoneGate son vulnerables.

Symantec

Los productos de Symantec Corporation no son vulnerables a este problema. Symantec no implementa SIP en ninguno de sus productos.

Xerox

Xerox esta conciente de esta vulnerabilidad y esta evaluando actualmente todos sus productos. Xerox actualizará esta información cuando las pruebas sean finalizadas.

APÉNDICE B.- Referencias

1. http://www.ee.oulu.fi/research/ouspg/protos/
2.

2. http://www.kb.cert.org/vuls/id/528719
3. http://www.cert.org/tech_tips/denial_of_service.html
4. http://www.ietf.org/html.charters/sip-charter.html
5. RFC3261 - SIP: Session Initiation Protocol
6. RFC2327 - SDP: Session Description Protocol
7. RFC2279 - UTF-8, a transformation format of ISO 10646
8. Session Initiation Protocol Basic Call Flow Examples
9. Session Initiation Protocol Torture Test Messages, Draft

El **Departamento de Seguridad en Cómputo/UNAM-CERT** agradece el apoyo en la elaboración, revisión y traducción de éste boletín a:

- José Inés Gervacio Gervacio (jgervaci@seguridad.unam.mx).
- Fernando Zaragoza Hernández (fzaragoz@seguridad.unam.mx).
- Edgar Cristobal Ramírez Miranda (eramirez@seguridad.unam.mx).

INFORMACIÓN

Éste documento se encuentra disponible en su formato original en la siguiente dirección:

http://www.cert.org/advisories/CA-2003-06.html

Para mayor información acerca de éste boletín de seguridad contactar a:

UNAM CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Computo
DGSCA - UNAM
E-Mail : seguridad@seguridad.unam.mx
http://www.unam-cert.unam.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel : 56 22 81 69
Fax : 56 22 80 43