UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−008

Gusano telnet para SUN Solaris

Un gusano se encuentra explotando una vulnerabilidad en el demonio telnet de Sun Solaris

Fecha de Liberación: 1 de Marzo de 2007

Ultima Revisión: 1 de Marzo de 2007

Fuente: CERT/CC

CVE ID: **CVE−2007−0882**

Riesgo

Altamente Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Acceso remoto al sistema

I. Sistemas Afectados

- Sun Solaris 10 (SunOS 5.10)
- Sun "Nevada" (SunOS 5.11)

Ambas arquitecturas son afectadas, SPARC e Intel (x86)

II. Descripción

Un gusano se encuentra explotando una vulnerabilidad en el demonio telnet (in.telnetd) de sistemas Sun Solaris no actualizados. La vulnerabilidad permite que el gusano (o cualquier intruso) tenga acceso al sistema vía telnet (23/tcp) con privilegios. Más detalles respecto a esta vulnerabilidad se encuentran disponibles por medio de las notas de la vulnerabilidad VU#881872 (CVE−2007−0882).

Debido a la facilidad para explotar la vulnerabilidad VU#881872 y a que existe publicada información técnica respecto a ella, no nada más el gusano, sino

cualquier intruso podría explotar esta vulnerabilidad.

Las características de esta vulnerabilidad son, pero no se limitan a:

- Explotar la vulnerabilidad VU#881872 para acceder vía telnet como usuario adm o lp
- Cambio de permisos en /var/adm/wtmpx a −rw−r−−rw−
- Crear el directorio .adm en /var/adm/sa/
- Agregar archivos .profile a /var/adm/ y /var/spool/lp/
- Instalar un shell como puerta trasera en el puerto 32982/tcp
- Modificar el acceso al crontab para los usuarios adm y lp
- Scaneo de otros sistemas que se encuentren ejecutando telnet (23/tcp)

Sun ha publicado la información del gusano en su sistema de alertas de seguridad incluyendo un script que deshabilita el demonio telnet y revierto los cambios realizado por el gusano.

III. Impacto

La vulnerabilidad VU#881872 permite que un intruso pueda acceder al sistema de forma remota en sistemass vulnerables vía telnet y obtener privilegios de administrador. El gusano aprovecha esta vulnerabilidad para comprometer equipos tal como se describe arriba. A partir de que el gusano instala un shell como puerta trasera, es posible que un intruso con conocimientos sobre el proceso de autenticación pueda acceder al sistema y realizar cualquier acción con privilegios de usuario adm o lp.

IV. Solución

Instalación de actualización

Para tratar la vulnerabilidad VU#881872, aplicar las actualizaciones adecuadas referentes a la alerta de seguridad 102802 de SUN.

Ejecución de script

Para restaurar los sistemas comprometidos, SUN ha publicado un script que deshabilita el demonio telnet y revierte los cambios que el gusano realiza. Es importante resaltar que este script sólo restaura los cambios que realiza este gusano. Al ejecutar el script, no se garantiza la integridad del sistema. Un sistema puede ser vulnerable de diferentes formas: un intruso puede explotar la vulnerabilidad VU#881872 o utilizar una puerta trasera instalada por el gusano. Para hacer una restauración completa, será necesario reinstalar el sistema comprometido utilizando software obtenido de fuentes confiables.

V. Medidas

Hasta que se apliquen las actualizaciones correspondientes, se de considerat las siguientes medidas:

Deshabilitar telnet

El demonio de telnet puede deshabilitarse haciendo uso de los siguientes comandos como usario root

```
# /usr/sbin/svcadm disable telnet
```

Restringir el acceso a telnet

Restringir el acceso a telnet (23/tcp) a redes no confiables tales como Internet

Usar SSH en lugar de telnet

SSH comparado con telnet, hace uso de un método más seguro para la autenticación remota. De forma general, se recomienda usar SSH en lugar de telnet.

VI. Referencias

- US−CERT Vulnerability Note VU#881872 − http://www.kb.cert.org/vuls/id/881872
- Recovering from an Incident − http://www.cert.org/nav/recovering.html
- Sun Alert Notification 102802 − http://sunsolve.sun.com/search/document.do?assetkey=1−26−102802−1
- Solaris in.telnetd worm seen in the wild + inoculation script − http://blogs.sun.com/security/entry/solaris_in_telnetd_worm_seen
- inoculate.local − http://blogs.sun.com/security/resource/inoculate.local
- CVE−2007−0882 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2007−0882

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

- Israel Becerril Sierra (ibecerril at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

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