BOLETÍN DE ALERTA

Boletín Nro.: 2016-04
Fecha de publicación: 20/01/2016
Tema: Vulnerabilidad de escalación de privilegios local en kernel de Linux

Sistemas afectados:

Kernel de Linux 3.8 y versiones superiores, así como los productos basados en las mismas

Algunas de las distribuciones del Linux afectadas:

- Red Hat Enterprise Linux 7
- CentOS Linux 7
- Debian Linux stable 8.x (jessie)
- Debian Linux testing 9.x (stretch)
- SUSE Linux Enterprise Desktop 12
- SUSE Linux Enterprise Desktop 12 SP1
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Workstation Extension 12
- SUSE Linux Enterprise Workstation Extension 12 SP1
- Ubuntu Linux 14.04 LTS (Trusty Tahr)
- Ubuntu Linux 15.04 (Vivid Vervet)
- Ubuntu Linux 15.10 (Wily Werewolf)
- Opensuse Linux LEAP and version 13.2
- La mayoría de las versiones de Android 4.0 (KitKat) y superiores

Descripción:

Se ha descubierto una vulnerabilidad crítica (CVE-2016-0728) que afecta a ciertas versiones del kernel de Linux la cual podría permitir a un atacante obtener privilegios de root en un dispositivo vulnerable.

La vulnerabilidad se debe a una pérdida de referencia en la utilidad de gestión de cadena de claves de Linux. Esta utilidad es, principalmente, una forma en la que las interfaces mantienen y almacenan temporalmente los datos de inicio de sesión, claves de autenticación, claves de cifrado, certificados y otros datos, y luego ponerlos a disposición de las aplicaciones.

Esta fuga de información de referencia podría ser explotada por un atacantes para ejecutar código arbitrario en el kernel de Linux. En una prueba de concepto llevado a cabo por los investigadores, ha tomado alrededor de 30 minutos en ejecutar exitosamente el exploit, hasta lograr escalar de privilegios.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

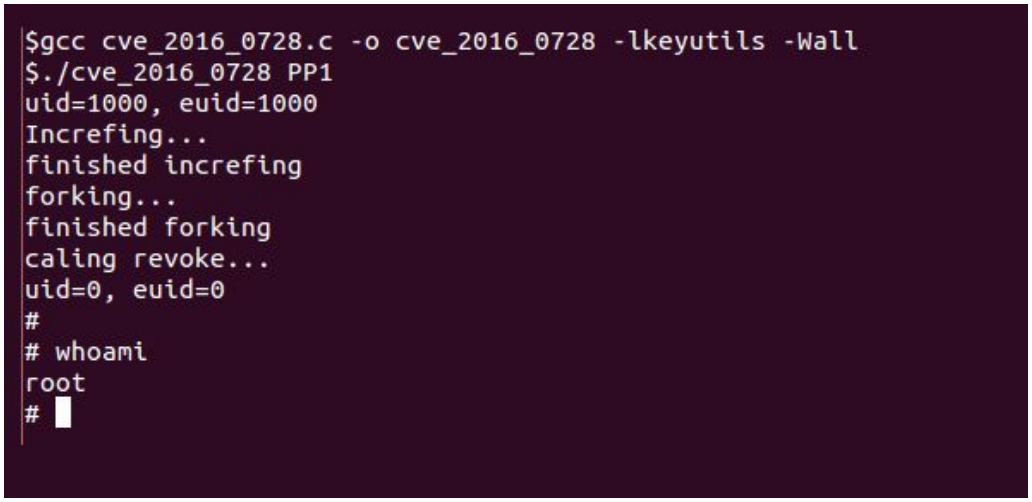

Figura 1: Explotación exitosa de la vulnerabilidad CVE-2016-0728

La vulnerabilidad estuvo presente en el código desde 2012, y afecta a cualquier sistema operativo con kernel Linux 3.8 y superior, por lo que se calcula que decenas de millones de ordenadores, tanto de 32 bits y 64 bits, se encuentran expuestos a esta falla. Además, afecta también a las versiones de Android KitKat y superior, lo que significa alrededor del 66% de todos los dispositivos Android también están expuestos a dicha vulnerabilidad.

Las vulnerabilidades fueron reportadas por el equipo de investigadores de Perception Point. Puede encontrar los detalles en el siguiente enlace:

http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

Impacto

Un atacante con acceso local a un sistema vulnerable puede escalar de privilegios y obtener permisos de root en el sistema operativo, lo que les permite un control total del mismo.

Solución

Se ha publicado un parche que corrige la vulnerabilidad del kernel de Linux. Las diferentes distribuciones de Linux también han publicado parches, en su mayoría. Se recomienda la actualización de los sistemas operativos afectados, siguiendo para ello las instrucciones específicas de cada distribución.

Debido a que se trata de una actualización a nivel de kernel, se debe reiniciar el sistema de modo a que los cambios sean aplicados.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Debian y Ubuntu:

```
$ sudo apt-get update && sudo apt-get upgrade && apt-get dist-upgrade
$ sudo reboot
```

Centos y Red Hat Enterprise Linux:

```
$ sudo yum update
$ reboot
```

En el caso de dispositivos Android, la actualización dependerá del fabricante y de la operadora, por lo que podría no estar disponible en todos los teléfonos. Para actualizar, se debe ingresar a la configuración del teléfono > "Acerca de.." > "Actualización del sistema". Las instrucciones específicas pueden variar de acuerdo a cada modelo de teléfono.

Figura 2: Ejemplo de actualización en Android

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Información adicional:

http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0728

https://security-tracker.debian.org/tracker/CVE-2016-0728

https://access.redhat.com/articles/2131021

https://access.redhat.com/security/cve/CVE-2016-0728

http://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-0728.html

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py