BOLETÍN DE ALERTA

Boletín Nro.: 2014-05

Fecha de publicación: 25/09/2014

Tema: Vulnerabilidad de Ejecución de Código Remoto en BASH

Sistemas afectados:
Basados en UNIX que incluyen Bourne Again Shell (BASH)

Descripción:

Se ha descubierto una vulnerabilidad crítica en el intérprete de comandos Bash (Bourne Again Shell) que permite la ejecución remota de código. La vulnerabilidad afecta a sistemas operativos basados en UNIX, tales como Linux y Mac OS X.
Es común que muchos programas ejecuten bash shell en segundo plano. Frecuentemente es utilizado para proveer un interprete de comandos a usuarios remotos (por ejemplo vía ssh, telnet, etc), un *parser* para scripts CGI (presentes en servidores web Apache, por ejemplo), para ofrecer un soporte limitado de ejecución de comandos.
Las variables de entorno de un sistema proporcionan una manera de influir en el comportamiento de un programa en un sistema. Estas variables de entorno pueden ser construidas con valores determinados antes de la llamada al *bash*. La vulnerabilidad permite incluir código en dichas variables, de modo que ese código es ejecutado cuando se llama al Bash.
A pesar de que Bash no es utilizado directamente por usuarios remotos, es una herramienta común para la ejecución de otros programas tales como servidores web o servidores de mail. Si la aplicación realiza llamadas a Bash a través de peticiones HTTP o de CGI y el usuario puede insertar datos, el servidor puede ser comprometido.

Impacto:
A través de la explotación de dicha vulnerabilidad es posible ejecutar código malicioso en el equipo, pudiendo obtenerse información confidencial, inyectar shells, entre otras posibilidades. Esta vulnerabilidad es especialmente critica debido a que Bash puede ser llamado de diversas maneras por una aplicación.

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
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

Detección:

Para determinar si un sistema es vulnerable, se puede ejecutar los siguientes comandos:
~# env X="() { :;} ; echo vulnerable" /bin/sh -c "echo completed"
~# env X="() { :;} ; echo vulnerable" `which bash` -c "echo completed"

Si en la salida se imprime “vulnerable”, el bash presenta la vulnerabilidad.

Solución:
Se han publicado actualizaciones de Bash para muchas de las distribuciones de sistemas operativos:

- Red Hat Enterprise Linux (version 4 a 7)
- Fedora
- CentOS
- Ubuntu 10.04 LTS, 12.04 LTS y 14.04 LTS
- Debian

Se recomienda aplicar las actualizaciones en la brevedad posible.
En caso de que no exista todavía actualización para su sistema operativo, se recomienda desactivar cualquier script CGI que realice llamadas a Bash. Si bien esto no representa una solución completa, ayudara a mitigar uno de los posibles vectores de ataque.

Información adicional:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

http://seclists.org/oss-sec/2014/q3/649

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
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