Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-009 Bash shell GNU ejecuta comandos en variables de entorno

GNU Bash 4.3 y las versiones anteriores contienen una vulnerabilidad de inyección de comandos que podría permitir la ejecución remota de código.

- **Fecha de Liberación:** 24-Sep-2014
- **Ultima Revisión:** 26-Sep-2014
- **Fuente:** cert.org
- **CVE ID:** VU#252743
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

1. ## Descripción

   CWE-78: Inyección de comandos

   Bash soporta la exportación de funciones de shell a otras instancias de bash usando una variable de entorno. Esta variable de entorno recibe su nombre del nombre de la función y comienza con "() {" como el valor de la variable en la definición de la función. Cuando Bash llega al final de la definición de función, en lugar de terminar la ejecución continúa procesando comandos de shell escritos después del final de la función. Esta vulnerabilidad es especialmente crítica porque Bash es muy utilizado en muchos tipos de dispositivos (sistemas operativos tipo UNIX, incluyendo Linux, BSD y Mac OS X), y debido a que muchos servicios de red utilizan Bash, haciendo que la vulnerabilidad sea explotable desde la red.

   Red Hat desarrolló la siguiente prueba:

   $ env x='() { :;}; echo vulnerable' bash -c "echo esto es una prueba"
2. ## Impacto

   Un atacante podría ejecutar código arbitrario con el nivel de privilegios de la aplicación que manda llamar a la variable de entorno.
3. ## Solución

   Aplicar una actualización

   El primer conjunto de parches (para CVE-2014-6271) no resuelven por completo la vulnerabilidad. CVE-2014-7169 identifica los aspectos restantes de esta vulnerabilidad. Red Hat ha proporcionado un artículo de soporte con soluciones provisionales.

   Sistemas operativos con actualizaciones disponibles:

   - CentOS

- Debian
- Redhat
- Ubuntu

4. Información de Proveedores

Muchos sistemas operativos tipo UNIX, incluyendo las distribuciones de Linux, variantes BSD, y Apple Mac OS X incluyen Bash y es probable que sean vulnerables. Comuníquese con su proveedor para obtener información acerca de las actualizaciones o parches. Este artículo de soporte de Red Hat (en inglés) y esta entrada de blog (en inglés) describen las formas en las que se puede llamar a Bash desde otros programas, incluyendo los vectores de red tales como CGI, SSH, y DHCP.

Proveedor	Estado	Fecha de Notificación	Fecha de Actualización
Apple Inc.	Afectado	25 Sep 2014	25 Sep 2014
Debian GNU/Linux	Afectado	25 Sep 2014	25 Sep 2014
Fedora Project	Afectado	25 Sep 2014	25 Sep 2014
GNU Bash	Afectado	-	25 Sep 2014
Juniper Networks, Inc.	Afectado	25 Sep 2014	25 Sep 2014
Oracle Corporation	Afectado	25 Sep 2014	25 Sep 2014
Red Hat, Inc.	Afectado	25 Sep 2014	25 Sep 2014
Slackware Linux Inc.	Afectado	25 Sep 2014	25 Sep 2014
ACCESS	Desconocido	25 Sep 2014	25 Sep 2014
Alcatel-Lucent	Desconocido	25 Sep 2014	25 Sep 2014
AT&T	Desconocido	25 Sep 2014	25 Sep 2014
Avaya, Inc.	Desconocido	25 Sep 2014	25 Sep 2014
Barracuda Networks	Desconocido	25 Sep 2014	25 Sep 2014
Belkin, Inc.	Desconocido	25 Sep 2014	25 Sep 2014
Blue Coat Systems	Desconocido	25 Sep 2014	25 Sep 2014

5. Referencias

http://seclists.org/oss-sec/2014/q3/650
https://access.redhat.com/articles/1200223
https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack
http://seclists.org/oss-sec/2014/q3/688
http://seclists.org/oss-sec/2014/q3/685
http://lcamtuf.blogspot.com/2014/09/quick-notes-about-bash-bug-its-impact.html

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Lilia Elena Gonzalez Medina (lgonzalez at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at 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 47