# ALERTE

**Vulnérabilité dite 'Shellshock' de *GNU Bourne Again Shell* (Bash) (CVE-2014-6271, CVE-2014-7169)**

## Systèmes affectés

- GNU Bash jusqu'à version 4.3.
- Linux, BSD, et distributions UNIX  y compris mais sans être exhaustif :
  - CentOS 5 à 7
  - Debian
  - Mac OS X
  - Red Hat Enterprise Linux 4 à 7
  - Ubuntu  10.04 LTS, 12.04 LTS, and 14.04 LTS

## Aperçu

Une vulnérabilité critique a été rapportée sur le shell GNU Bourne Again Shell (Bash), le shell le plus utilisé dans la plus part des systèmes d'exploitation Linux/UNIX et Mac OS X d'Apple.  Plusieurs analystes et d'organismes de sécurité ont rapporté la découverte d'une exploitation massive de cette faille à des fins malveillantes.

## Description

Les versions 1.14 à 4.3 de GNU Bash contiennent une faille qui traite des commandes placées après les définitions de fonction dans une variable d'environnement ajoutée, permettant à des attaquants distants d'exécuter un code arbitraire via un environnement forgé qui active une exploitation à partir du réseau.

## Impact

Cette vulnérabilité est classée par les standards de l'industrie au niveau d'impact "haut" avec un score CVSS de 10 et niveau « bas » en termes de complexité, ce qui signifie qu'il requiert un faible niveau de compétence pour l'exploiter. La faille permet des à attaquants de fournir notamment des variables d'environnement forgés contenant des commandes arbitraires qui peuvent être exécutés sur des systèmes vulnérables. Cela est particulièrement dangereux à cause de l'utilisation répandue du shell Bash et de sa faculté  à être appelé par une application par divers moyens.

## Diagnostic

Pour vérifier si la version du Bash que vous utilisez est touchée par cette vulnérabilité, exécutez la commande suivante :

```
$ env x='() { :;}; echo vulnerable'  bash -c "echo ceci est un test"
```

Si la sortie de la commande ci-dessus ressemble à ce qui suit :

```
vulnerable
ceci est un test
```

alors vous utilisez une version de Bash vulnérable.

Si la même commande exécutée retourne un résultat comme suit :

```
$ env x='() { :;}; echo vulnerable'  bash -c "echo ceci est un test"
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
ceci est un test
```

alors vous utilisez une version corrigée de Bash.

Vous pouvez également déterminer la version de votre Bash et vérifier si elle figure dans la liste des versions affectées publiée par votre éditeur. Pour connaitre la version du bash installé :

```
$ bash –version
```

## Solution

Des correctifs ont été publiés par de nombreux éditeurs de Linux pour les versions affectées. Les solutions pour le CVE-2014-6271 ne résolvent pas complètement la vulnérabilité. Il est conseillé d'installer des correctifs et faire attention à les mettre à jour pour prendre en compte aussi CVE-2014-7169.

Beaucoup de Bash de systèmes d'exploitation de type-Unix, y compris les distributions Linux, les variantes de BSD et Mac OS X d'Apple sont susceptibles d'être affectés. Referez-vous à votre éditeur pour des informations de mise-à-jour. Une liste d'éditeurs peut être trouvée dans la Note de Vulnérabilité VU#252743 du CERT/CC.

BF-CIRT recommandes aux administrateurs systèmes de prendre connaissance des correctifs des éditeurs et de consulter la synthèse de la vulnérabilité publiée par NIST CVE-2014-7169, afin d'atténuer les dégâts d'une exploitation.

## Références


- DHS NCSD; Vulnerability Summary for CVE-2014-6271
- DHS NCSD; Vulnerability Summary for CVE-2014-7169
- Red Hat, Bash specially-crafted environment variables code injection attack
- CERT Vulnerability Note VU#252743
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-006/index.html
- https://www.us-cert.gov/ncas/alerts/TA14-268A
- https://access.redhat.com/articles/1200223


## Révisions

- 26 septembre 2014 – Date de première publication

Retour haut de page

Computer Incidents Response Team (CIRT)
01 BP 6437 Ouagadougou 01
Tel : +226 50 37 53 60/61/62 Poste 284 – Fax : +226 50 37 53 64 – Email : cirt@cirt.bf –
Signalement d'incidents : incidents@cirt.bf
Site Web : http://www.cirt.bf