Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 25 septembre 2014
N° CERTFR-2014-ALE-006

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans GNU bash

Gestion du document

Référence	CERTFR-2014-ALE-006
Titre	Vulnérabilité dans GNU bash
Date de la première version	25 septembre 2014
Date de la dernière version	30 septembre 2014
Source(s)	Bulletin de sécurité Debian DSA-3032-1 du 24 septembre 2014 Bulletin de sécurité Debian DSA-3035-1 du 25 septembre 2014 Bulletin de sécurité Ubuntu USN-2362-1 du 24 septembre 2014 Bulletin de sécurité Ubuntu USN-2363-1 du 25 septembre 2014 Bulletin de sécurité Ubuntu USN-2363-2 du 25 septembre 2014 Bulletin de sécurité Ubuntu USN-2364-1 du 27 septembre 2014 Bulletin de sécurité RedHat du 24 septembre 2014 Bulletin de sécurité RedHat du 26 septembre 2014
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance

2 - Systèmes affecté(s)

- Bash versions antérieures au 25 septembre 2014
- GNU Bash 3.0 versions antérieures à 3.0.17
- GNU Bash 3.1 versions antérieures à 3.1.18
- GNU Bash 3.2 versions antérieures à 3.2.52
- GNU Bash 4.0 versions antérieures à 4.0.39
- GNU Bash 4.1 versions antérieures à 4.1.12
- GNU Bash 4.2 versions antérieures à 4.2.48
- GNU Bash 4.3 versions antérieures à 4.3.25
- Bash Debian Squeeze versions antérieures à 4.1-3+deb6u2
- Bash Debian Wheezy versions antérieures à 4.2+dfsg-0.1+deb7u3

- Bash Ubuntu 14.04 LTS versions antérieures à 4.3-7ubuntu1.3
- Bash Ubuntu 12.04 LTS versions antérieures à 4.2-2ubuntu2.3
- Bash Ubuntu 10.04 LTS versions antérieures à 4.1-2ubuntu3.2
- Bash Red Hat Enterprise Linux 7 versions antérieures à bash-4.2.45-5.el7_0.4
- Bash Red Hat Enterprise Linux 6 versions antérieures à bash-4.1.2-15.el6_5.2, bash-4.1.2-15.el6_5.1.sjis.1, bash-4.1.2-9.el6_2.1, bash-4.1.2-15.el6_4.1
- Bash Red Hat Enterprise Linux 5 versions antérieures à bash-3.2-33.el5_11.4, bash-3.2-33.el5_11.1.sjis.1, bash-3.2-24.el5_6.1, bash-3.2-32.el5_9.2
- Bash Red Hat Enterprise Linux 4 versions antérieures à bash-3.0-27.el4.2

3 - Résumé

Une vulnérabilité a été découverte dans *GNU bash*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Solution

La vulnérabilité CVE-2014-6271 consiste en une injection de commande suivant la définition d'une fonction dans une variable d'environnement. Dans certains cas, un processus peut hériter de variables d'environnement provenant d'une machine distante, ce qui rend cette vulnérabilité exploitable à distance. C'est notamment le cas de serveurs Web employant des scripts bash comme CGI-bin, de certains serveurs SSH et des clients DHCP.

Il est possible de vérifier si la version de bash est vulnérable avec la commande:

```
$ env VAR='() { 0; }; echo danger'  bash -c "echo bonjour"
```

A l'heure actuelle, certains correctifs sont incomplets en raison d'une vulnérabilité résiduelle (CVE-2014-7169). Néanmoins le CERT-FR recommande d'appliquer les correctifs pour réduire la facilité d'exploitation. Les derniers correctifs des distributions Debian, Ubuntu et RedHat corrigent aussi CVE-2014-7169.

5 - Documentation

- Bulletin de sécurité Debian DSA-3032-1 du 24 septembre 2014
  http://www.debian.org/security/2014/dsa-3032
- Bulletin de sécurité Debian DSA-3035-1 du 25 septembre 2014
  http://www.debian.org/security/2014/dsa-3035
- Bulletin de sécurité Ubuntu USN-2362-1 du 24 septembre 2014
  http://www.ubuntu.com/usn/usn-2362-1/
- Bulletin de sécurité Ubuntu USN-2363-1 du 25 septembre 2014
  http://www.ubuntu.com/usn/usn-2363-1/
- Bulletin de sécurité Ubuntu USN-2363-2 du 25 septembre 2014
  http://www.ubuntu.com/usn/usn-2363-2/
- Bulletin de sécurité Ubuntu USN-2364-1 du 27 septembre 2014
  http://www.ubuntu.com/usn/usn-2364-1/
- Bulletin de sécurité RedHat du 24 septembre 2014
  https://access.redhat.com/articles/1200223
- Bulletin de sécurité RedHat du 26 septembre 2014
  https://rhn.redhat.com/errata/RHSA-2014-1306.html
- Référence CVE CVE-2014-6271
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
- Référence CVE CVE-2014-6277
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6277
- Référence CVE CVE-2014-6278
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278
- Référence CVE CVE-2014-7169
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

- Référence CVE CVE-2014-7186
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7186
- Référence CVE CVE-2014-7187
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7187

Gestion détaillée du document

25 septembre 2014 version initiale.
26 septembre 2014 mise à jour.
29 septembre 2014 mise à jour.
30 septembre 2014 mise à jour.