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 26 septembre 2014
N° CERTFR-2014-ACT-039

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-039

1 - Vulnérabilités critiques sur bash - CVE-2014-6271 / CVE-2014-7169

Le 24 septembre 2014, une mise à jour critique de `bash` a été proposée par de nombreuses distributions Linux, suite à la découverte d'une vulnérabilité de type injection de code à distance.

Cette dernière a été utilisée à des fins malveillantes, en particulier dans des reconnaissances de réseaux ainsi que pour propager des codes malveillants. Cette vulnérabilité a fait l'objet de l'alerte CERTFR-2014-ALE-006 datée du 25 septembre.

Détails de la vulnérabilité

Le *Bourne Again Shell*, plus connu sous le nom de `bash`, est un interpréteur de commandes (shell) largement déployé sur la majorité des systèmes Unix.

La vulnérabilité (CVE-2014-6271) réside dans le traitement des fonctions déclarées au sein de variables d'environnement. Bash permet en effet de définir des fonctions directement au sein de variables d'environnement.

Le problème initial se situait dans la possibilité d'exécuter du code supplémentaire qui était mis à la suite de la déclaration de la fonction dans la variable d'environnement.

Un correctif a été intégré par les principales distributions Linux le 24 septembre, toutefois le chercheur en sécurité Tavis Ormandy a montré que celui-ci était incomplet et qu'une vulnérabilité résiduelle (CVE-2014-7169) demeurait via une autre définition spécifique de la fonction au sein de la variable d'environnement. Cette seconde vulnérabilité permet l'écriture d'un fichier arbitraire.

Un correctif corrigeant les deux vulnérabilités a été poussé pour la majorité des distributions Linux le 26 septembre.

Systèmes affectés

Bash étant exposé à de potentiels utilisateurs malveillants par de nombreuses applications, l'impact global de cette vulnérabilité n'est pas encore connu. Toutefois, il est possible de dresser une liste de services vulnérables identifiés à ce jour :

- Apache, lors de l'activation de `mod_cgi`, lorsque les scripts CGI utilisés sont des scripts shells, ou lorsque les scripts font des appels implicites à `bash`, par exemple via des fonctions comme `popen()` ou `system()` ;
- certains clients DHCP utilisant des variables d'environnement peuvent être vulnérables en cas de serveur DHCP malveillant ;
- les shells restreints en SSH, mais uniquement après authentification, ce qui limite le risque d'exploitation de la vulnérabilité ;
- n'importe quelle application exportant des variables d'environnement lors de la création de sous-processus via `bash`, et en particulier les binaires `setuid`.

Conclusion

Face à cette vulnérabilité critique, le CERT-FR recommande à tous les administrateurs et responsables de systèmes Unix comportant le shell `bash` de mettre à jour rapidement leurs systèmes afin d'éviter une compromission.

Documentation

– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-006/

2 - Publication du rapport de l'Observatoire de la résilience de l'Internet

Le rapport portant sur l'année 2013 de l'Observatoire de la résilience de l'Internet français vient d'être publié. Il est issu des travaux de recherche de l'ANSSI effectués avec la collaboration de l'Afnic sur l'usage des protocoles BGP et DNS par les opérateurs français.

Ces protocoles permettent aux réseaux, opérés par des fournisseurs d'accès (FAI) et des fournisseurs de contenu, de s'interconnecter pour former l'Internet. La résilience est définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Une extension naturelle en est la robustesse, c'est-à-dire la capacité à limiter au maximum les impacts d'un incident. L'étude menée à ce titre montre que tous les opérateurs français possédant au moins deux fournisseurs peuvent continuer à joindre le reste de l'Internet en cas de panne de n'importe quel autre opérateur.

Outre ses conclusions rassurantes sur la situation de l'Internet français, l'Observatoire publie dans son rapport une introduction aux protocoles RPKI et DNSSEC dont l'adoption contribuera à la sécurisation d'Internet, et émet les recommandations suivantes:

– déployer IPv6 afin de développer rapidement les compétences, et d'anticiper les problèmes opérationnels futurs ;
– bien répartir les serveurs DNS faisant autorité afin d'améliorer la robustesse de l'infrastructure ;
– tester DNSSEC et le déployer pour lutter contre les attaques par pollution de cache ;
– déclarer systématiquement les objets route, et les maintenir à jour, afin de faciliter la détection et le filtrage d'annonces BGP illégitimes ;
– utiliser la RPKI et déclarer des ROA ;
– appliquer les bonnes pratiques BGP au niveau des interconnexions entre opérateurs.

L'ANSSI encourage les acteurs de l'Internet à s'approprier ces recommandations pour les appliquer au mieux et au plus tôt.

Documentation

– http://www.ssi.gouv.fr/observatoire
– http://www.ssi.gouv.fr/IMG/pdf/guide_configuration_BGP.pdf

3 - Sauvegarde des données mobiles et risques

Les données stockées sur les téléphones portables professionnels, comme toute donnée du système d'information, doivent faire l'objet de mesures de sécurité adaptées.

Il est particulièrement important de ne pas oublier le volet « Sauvegarde » de ces données, cette catégorie d'appareils étant plus susceptible de se retrouver égarée et/ou volée que d'autres types de matériels informatiques.

L'actualité récente nous rappelle la fragilité des solutions grand public de sauvegarde « dans le cloud », qui reposent souvent sur un mot de passe pour lequel aucune politique de robustesse n'est définie ; et qui stockera usuellement les données sur des espaces de stockages non maitrisés.

Le CERT-FR recommande l'utilisation de logiciels de gestion de flotte de terminaux mobiles lorsque ceux-ci sont utilisés au sein d'un environnement professionnel. Ils comportent généralement un volet « stratégie de sauvegarde » permettant de réaliser des archives régulières ; le CERT-FR recommande en particulier, lorsque c'est possible, de configurer cette fonctionnalité de sorte à placer les sauvegardes sur un serveur au sein de l'entité. Cela laissera les équipes chargées du SI gérer les incidents liés à ce type de matériels sereinement tout en limitant au mieux les risques pesant sur la confidentialité des données.

Documentation

- Recommandations de l'ANSSI relative aux ordiphones :
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-solutions-de-mobilite/recommandations-de-securite-relatives-aux-ordiphones.html

4 - Rappel des avis émis

Dans la période du 19 au 25 septembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-006 : Vulnérabilité dans GNU bash
- CERTFR-2014-AVI-394 : Multiples vulnérabilités dans Asterisk
- CERTFR-2014-AVI-395 : Multiples vulnérabilités dans les produits F5
- CERTFR-2014-AVI-396 : Multiples vulnérabilités dans le noyau Ubuntu
- CERTFR-2014-AVI-397 : Vulnérabilité dans les systèmes SCADA Schneider Electric
- CERTFR-2014-AVI-398 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2014-AVI-399 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2014-AVI-400 : Vulnérabilité dans Google Chrome
- CERTFR-2014-AVI-401 : Vulnérabilité dans les produits Mozilla
- CERTFR-2014-AVI-402 : Multiples vulnérabilités dans Xen

Gestion détaillée du document

26 septembre 2014 version initiale.