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 02 février 2015
N° CERTFR-2015-ACT-005

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-005

1 - Retour sur la vulnérabilité GHOST

Contexte

Le 17 janvier 2015, un message posté sur un forum de discussion français (1) révèle une vulnérabilité découverte par la société Qualys (2) concernant la bibliothèque `glibc`.

Cette vulnérabilité impacte la fonction `__nss_hostname_digits_dots` (utilisée par la famille de fonctions de type `gethostbyname*`) et a été introduite à la fin des années 90. Corrigée le 21 mai 2013 par les développeurs du projet `glibc`, cette mise à jour a été intégrée dans toutes les distributions "récentes" de Linux.

Cependant, ce correctif n'avait pas été porté sur les versions LTS (Long Term Support ou support étendu) par les mainteneurs, car il avait été jugé comme ne relevant pas d'une mise à jour de sécurité. En effet, dans ce type de distribution, seules les mises à jour de sécurité sont portées. En particulier, les distributions suivantes sont impactées :

- Debian 7 ;
- Red Hat EL 6 et 7 ;
- Ubuntu 12.04.

Depuis la publication de cette vulnérabilité, ces distributions ont procédé au portage du correctif sur leurs différentes versions LTS :

- http://people.canonical.com/ ubuntu-security/cve/2015/CVE-2015-0235.html ;
- https://security-tracker.debian.org/tracker/CVE-2015-0235 ;
- https://access.redhat.com/security/cve/CVE-2015-0235 .

Analyse de la vulnérabilité

La vulnérabilité porte sur une fonction interne de `glibc`, accessible au travers d'appels aux fonctions `gethostbyname` et `gethostbyname2`. Il est à noter que ces fonctions sont dépréciées comme l'indique la documentation : "gethostbyname*() et gethostbyaddr*() sont déconseillées. Les applications devraient utiliser getaddrinfo(3) et getnameinfo(3) à la place."

Concernant la vulnérabilité en elle même, il s'agit d'un débordement de tampon (de 4 à 8 octets selon l'architecture utilisée) dans le tas. Ce débordement est dû à l'oubli d'un élément lors du calcul de l'espace nécessaire à la copie de données.

```
size_needed = (sizeof (*host_addr) + sizeof (*h_addr_ptrs) + strlen (name) + 1);

size_needed = (sizeof (*host_addr) + sizeof (*h_addr_ptrs)
+ sizeof (*h_alias_ptr) + strlen (name) + 1);
```

Lors du positionnement des éléments dans l'espace mémoire alloué, l'élément `h_alias_ptr` n'a pas sa place "réservée" et est donc situé à l'emplacement des 4 (ou 8 selon l'architecture) premiers octets de l'élément `hostname`.

Si `hostname` atteint sa taille maximale, alors le débordement est réalisé, comme présenté ci-dessous :

```
host_addr = (host_addr_t ) *buffer;
h_addr_ptrs = (host_addr_list_t *) ((char *) host_addr + sizeof (*host_addr));
h_alias_ptr = (char *) ((char *) h_addr_ptrs + sizeof (*h_addr_ptrs));
hostname = (char *) h_alias_ptr + sizeof (*h_alias_ptr);
```

Afin de déclencher ce débordement, le nom d'hôte doit remplir certaines conditions :

- le premier caractère du nom d'hôte doit être un chiffre ;
- le dernier caractère du nom d'hôte ne doit pas être un point ;
- le nom d'hôte ne doit contenir que des chiffres et des points ;
- le nom d'hôte doit être suffisamment long pour pouvoir dépasser la taille du tampon alloué ;
- le nom d'hôte doit pouvoir être interprété par la fonction `__inet_aton`, dans le cas d'une adresse ipv4, et par la fonction `__inet_pton`, dans le cas d'une adresse ipv6.

Dans le cas d'une adresse de type ipv6, le format même de ces adresses ne respecte pas la condition stipulant que le nom d'hôte ne doit contenir que des chiffres et des points, à cause de la présence du caractère ':' dans les adresses. Cette vulnérabilité ne peut donc pas être déclenchée par des appels à `gethostbyname2` avec en second paramètre `AF_INET6`.

Dans la plupart des cas, l'exploitation de cette vulnérabilité permet de réaliser un déni de service sur l'application vulnérable. Dans le cas du serveur mail Exim (en utilisant une configuration différente de celle par défaut), cette vulnérabilité peut, selon Qualys, provoquer une exécution de code arbitraire à distance par l'envoi de commandes forgées au serveur de messagerie.

Il semblerait que l'exploitation de cette vulnérabilité repose sur le fait que le programme utilise un gestionnaire d'allocation de mémoire interne qui, une fois corrompu, fournirait une primitive d'écriture arbitraire.

Toujours selon Qualys (3) les binaires suivants ne seraient pas affectés par cette vulnérabilité :

- apache ;
- cups ;
- dovecot ;
- gnupg ;
- isc-dhcp ;
- lighttpd ;
- mariadb/mysql ;
- nfs-utils ;
- nginx ;
- nodejs ;
- openldap ;
- openssh ;
- postfix ;
- proftpd ;
- pure-ftpd ;
- rsyslog ;
- samba ;
- sendmail ;
- sysklogd ;
- syslog-ng ;
- tcp_wrappers ;
- vsftpd ;
- xinetd.

Le CERT-FR recommande donc d'effectuer les dernières mises à jour proposées par les différentes distributions, ainsi que de redémarrer la machine après applications des correctifs.

Ce redémarrage permet de s'assurer que la version vulnérable de la glibc n'est plus utilisée par les processus.

Documentation :

- (1) :
  http://www.frsag.org/pipermail/frsag/2015-January/005722.html
- (2) :
  https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt
- (3) :
  http://www.openwall.com/lists/oss-security/2015/01/27/18

2 - Publication de recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows

Il y a deux semaines, l'ANSSI a publié une note technique sur des recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows.

Firefox est le navigateur web en source ouverte édité par la fondation Mozilla qui est devenu rapidement l'un des navigateurs les plus utilisés par les internautes. Il dispose d'un mécanisme de mise à jour automatique, peut être configuré de manière centralisée et possède un haut degré de paramétrage. Il se prête bien à une utilisation professionnelle et peut s'adapter à des environnements avec de fortes contraintes techniques.

Cette note a pour but de présenter :

- les enjeux de sécurité d'un navigateur Web ;
- les différences entre Firefox et Firefox ESR (« Extended Support Release ») ;
- des recommandations sur la configuration sécurisée du navigateur (choix des greffons et extensions, télé-déploiement initial et gestion des mises à jour) ;
- l'utilisation d'un mode "double navigateur" permettant de séparer des contextes d'utilisation (navigation / applications métier).

Des annexes détaillent les points suivants :

- stratégies de sécurisation de Firefox (liste de valeurs recommandées permettant de mettre en oeuvre les recommandations formulées dans cette note) ;
- déploiement et configuration centralisée dans un domaine Active Directory par GPP (« Global Policy Preferences ») ;
- déploiement et maîtrise des magasins de certificats des profils utilisateur Firefox ;
- télé-déploiement d'un module de recherche personnalisé par GPO (« Global Policy Object »).

http://www.ssi.gouv.fr/IMG/pdf/NP$_N avigateur Securise_F ire Fox.pdf$

3 - Rappel des avis émis

Dans la période du 26 janvier au 01 février 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-038 : Vulnérabilité dans les produits BlueCoat
- CERTFR-2015-AVI-039 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-040 : Multiples vulnérabilités dans Apple OS X
- CERTFR-2015-AVI-041 : Multiples vulnérabilités dans Apple Safari
- CERTFR-2015-AVI-042 : Multiples vulnérabilités dans Apple iOS
- CERTFR-2015-AVI-043 : Vulnérabilité dans glibc
- CERTFR-2015-AVI-044 : Multiples vulnérabilités dans VMware
- CERTFR-2015-AVI-045 : Vulnérabilité dans Cisco Prime Service Catalog
- CERTFR-2015-AVI-046 : Multiples vulnérabilités dans Asterisk
- CERTFR-2015-AVI-047 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-048 : Vulnérabilité dans VMware VDP

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2014-ALE-008 : Vulnérabilité dans Drupal (fermeture de l'alerte.)

- CERTFR-2014-ALE-010 : Vulnérabilité de l'implémentation des protocoles SSL/TLS dans Microsoft Windows (fermeture de l'alerte.)
- CERTFR-2014-ALE-011 : Vulnérabilité de l'implémentation Kerberos dans Microsoft Windows (fermeture de l'alerte.)
- CERTFR-2015-ALE-001 : Vulnérabilité dans Adobe Flash Player (fermeture de l'alerte.)

Gestion détaillée du document

02 février 2015 version initiale.