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 21 février 2014
N° CERTFR-2014-ACT-008

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-008

1 - Ingéniérie sociale et services de support informatique frauduleux

Le CERT-FR a constaté une recrudescence de techniques d'ingénierie sociale où un escroc se fait passer pour un agent appartenant à un service de support technique.

Deux méthodes principales sont le plus souvent employées pour contacter une victime potentielle :

- l'appel à froid (« *cold call* ») : un escroc appelle directement sa victime en prétendant être le technicien d'un service de support informatique. Il utilise alors des techniques d'ingénierie sociale en expliquant à la victime que son ordinateur est sujet à des comportements suspects ;
- la publicité en ligne : certains attaquants utilisent les moteurs de recherche pour référencer de fausses entreprises de support informatique. Un utilisateur à la recherche d'une solution à un problème technique sera ainsi tenté de rentrer en contact avec ces entreprises, notamment par téléphone.

Dans tous les cas, la victime est mise en confiance et incitée à payer pour une assistance ou un produit. Dans certains cas, le prétendu technicien peut également faire installer à l'utilisateur ciblé des logiciels de prise de contrôle à distance (tel que *LogMeIn*) sur ses équipements. Depuis peu, le même type d'escroquerie a été constaté pour les terminaux mobiles.

Les ficelles utilisées par les attaquants sont traditionnelles. Elles consistent à exploiter le manque de connaissances et la naïveté des victimes afin de prendre le contrôle de leur ordinateur ou de leur terminal. Certains cas d'escroquerie, utilisant notamment des codes malveillants de type « *ransomware* », font appel à du chantage afin de soutirer de l'argent aux victimes. Dans d'autres cas, l'escroquerie consiste à amener l'utilisateur à acheter un logiciel non malveillant mais ne remplissant pas ses fonctions (généralement un faux antivirus).

Un technicien de support informatique légitime n'est pas censé amener l'utilisateur à installer un quelconque outil supplémentaire sur un poste de travail, ni à lui demander d'identifiants et de mots de passe d'authentification.

Le CERT-FR recommande de:

- faire preuve de la plus grande prudence vis-à-vis des appels téléphoniques provenant de services de support alors que ceux-ci n'ont pas été sollicités ;
- solliciter, dans un cadre professionnel, uniquement les services de supports internes à l'entreprise ou à l'organisation.

2 - Analyse de la vulnérabilité CVE-2014-0038 affectant le noyau Linux

Rendue publique le 31 janvier 2014 [1], cette vulnérabilité offre la possibilité de modifier les données référencées par une adresse arbitraire au niveau du noyau Linux. Son exploitation permet une élévation de privilèges.

Cette vulnérabilité a été introduite, avec la version 3.4 du noyau Linux, par la modification de la fonction `compat_sys_recvmmsg` :

```
@@ -767,6 +777,11 @@ asmlinkage long compat_sys_recvmmsg(int fd,
                    struct compat_mmsghdr __user *mmsg, unsigned int vlen,
                    unsigned int flags, struct compat_timespec __user *timeout)
int datagrams;
struct timespec ktspec;
+ if (COMPAT_USE_64BIT_TIME)
+ return __sys_recvmmsg(fd, (struct mmsghdr __user *)mmsg, vlen,
+ flags | MSG_CMSG_COMPAT,
+ (struct timespec *) timeout);
+
if (timeout == NULL)
return __sys_recvmmsg(fd, (struct mmsghdr __user *)mmsg, vlen,
flags | MSG_CMSG_COMPAT, NULL);
```

En effet, lorsque la directive `COMPAT_USE_64BIT_TIME` est définie, un pointeur contrôlé par l'utilisateur (`struct compat_timespec __user *timeout`) est passé, sans aucune vérification sur sa valeur, à la fonction `__sys_recvmmsg`. Cette directive dépend de l'option de compilation `CONFIG_X86_X32` qui correspond à une nouvelle fonctionnalité du noyau 3.4 permettant aux binaires n'ayant pas besoin d'un espace d'adressage de 64 bits d'obtenir un espace réduit de 32 bits tout en étant capable d'utiliser des instructions spécifiques à l'architecture 64 bits. [2]

Les systèmes vulnérables sont donc :

- ceux basés sur une architecture 64 bits ;
- ceux dont la version du noyau est supérieure à 3.4.

La fonction vulnérable prend en paramètres un descripteur de fichier correspondant à une `socket` et un `timeout` qui est mis à jour lors de la réception d'un message. Cette mise à jour de la valeur pointée par `timeout` permet une écriture à une adresse arbitraire dans le noyau.

Les codes d'exploitation développés pour exploiter ce type de vulnérabilité font souvent appel à des charges utiles allouées dans une zone mémoire en espace utilisateur.

Des mesures de protection en profondeur apportées par la fonctionnalité `SMEP` des processeurs Intel (supportée depuis Linux 3.0 et Windows 8) ou l'option `PAX_MEMORY_UDEREF` de *grsecurity* peuvent empêcher ces codes de s'exécuter.

Cependant même si l'exécution de code en espace utilisateur n'est plus possible depuis le noyau, il existe d'autres méthodes d'exploitation, plus complexes à mettre en oeuvre, permettant de contourner ces protections.

C'est pourquoi le CERT-FR recommande, pour les systèmes vulnérables, d'appliquer les dernières mises à jour du noyau ou, si possible, de recompiler ce dernier sans l'option `CONFIG_X86_X32`.

Documentation

- Avis du CERT-FR concernant le noyau Linux d'Ubuntu :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-048
- Avis du CERT-FR concernant le noyau Linux de Mandriva :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-073
- Références :
  1 http://seclists.org/oss-sec/2014/q1/187
  2 http://www.phoronix.com/scan.php?page=news_itempx=MTA1OTY

3 - Rappel des avis émis

Dans la période du 14 au 20 février 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-001 : Vulnérabilité dans Microsoft Internet Explorer
- CERTFR-2014-AVI-070 : Vulnérabilité dans phpMyAdmin
- CERTFR-2014-AVI-071 : Vulnérabilité dans GnuTLS

- CERTFR-2014-AVI-072 : Multiples vulnérabilités dans Symantec Endpoint Protection Manager
- CERTFR-2014-AVI-073 : Multiples vulnérabilités dans le noyau Linux de Mandriva
- CERTFR-2014-AVI-074 : Vulnérabilité dans Xen
- CERTFR-2014-AVI-075 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-076 : Vulnérabilité dans Citrix ShareFile Mobile
- CERTFR-2014-AVI-077 : Multiples vulnérabilités dans Ruby On Rails

Gestion détaillée du document

21 février 2014 version initiale.