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 12 janvier 2015
N° CERTFR-2015-ACT-002

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-002

1 - Vulnérabilités sur le service ntpd

De multiples vulnérabilités affectant le logiciel *ntpd* ont été découvertes par Stephen Roettger et Neel Mehta, tous deux membres de l'équipe sécurité de Google.

Ces vulnérabilités affectent toutes les versions de ntpd antérieures à 4.2.8. Le logiciel ntpd est un démon qui agit en tant que client/serveur et qui permet, à travers le protocole NTP, de synchroniser l'horloge d'un système informatique avec celle d'un serveur dédié.

Les chercheurs ont identifié des vulnérabilités de type « dépassement de tampon » et des faiblesses dans la fonction de génération de clés aléatoires.

CVE-2014-9293

Le logiciel ntpd supporte un mécanisme d'authentification reposant sur une clé définie via la directive `keys` dans le fichier ntp.conf. Si cette directive n'est pas présente, une clé aléatoire de seulement 31 bits est générée, facilitant ainsi les attaques par force brute pour contourner l'authentification.

CVE-2014-9294

La graine d'initialisation du générateur de nombre aléatoire est basée sur l'heure système d'un serveur NTP alors qu'il est possible de récupérer celle-ci en envoyant une requête. Le paquet NTP reçu par un client comporte un champ `Receive Timestamp` qui a la valeur de l'heure système du serveur interrogé au moment où le paquet est envoyé au client. Il serait donc possible de faire une attaque par recherche exhaustive pour retrouver la graine.

Note : il est possible de forcer l'initialisation de la graine depuis un fichier spécifique en ajoutant la directive `crypto randfile` dans le fichier de configuration `/etc/ntp.conf`.

CVE-2014-9295

La fonction `ctl_putdata()` est vulnérable à un dépassement de tampon.

Cette fonction est utilisée pour écrire des données dans un paquet qui contient la réponse à une requête de type `control message` (utilisé par `ntpq` pour interroger le serveur NTP sur son état courant).

Si la taille des données à écrire est supérieure à la taille du tampon qui doit contenir ces données, la fonction `memmove()` sera utilisée, ce qui aura pour conséquence d'écraser le tampon (déclaré en global donc dans la section `.data`) et le reste des données de la section.

Une autre vulnérabilité de type « dépassement de tampon sur la pile » affecte la fonction `crypto_recv()` dans le fichier `ntp_crypto.c`. Cette vulnérabilité est exploitable uniquement lorsque l'authentification `autokey` est activée (toujours via le fichier ntp.conf).

Dans ce mode, le serveur distribue une valeur unique (« *cookie* ») par client. Lorsqu'il reçoit une requête, le serveur renvoie le cookie du client chiffré et les réponses sont signées en utilisant la clé privée de signature du serveur.

Pour déclencher la vulnérabilité, le paquet NTP reçu par le serveur doit passer toutes les vérifications faites dans la fonction `receive()` (vérification de la taille de la MAC, de la taille du champ d'extension, calcul de la somme de contrôle du paquet, etc).

La fonction incriminée réalise plusieurs vérifications pour savoir si le cookie reçu du client est valide : pour cela, elle va entre autre utiliser la fonction `RSA_private_decrypt()`.

```
if (vallen == (u_int)EVP_PKEY_size(host_pkey)) {
    if (RSA_private_decrypt(vallen,
        (u_char *)ep->pkt,
        (u_char *)&temp32,
        host_pkey->pkey.rsa,
        RSA_PKCS1_OAEP_PADDING) <= 0) {
            rval = XEVNT_CKY;
            break;
    } else {
    // ...

}
```

Cette fonction va déchiffrer les `vallen` octets (la taille maximale de la signature que la clé peut produire) situés à `ep->pkt` (qui correspond au champ `value` du champ extension du paquet NTP, qui est une valeur contrôlée par le client) et copier le contenu déchiffré à l'adresse `temp32` qui est une variable locale.

Une exploitation de la vulnérabilité pourrait donc écraser d'autres données sur la pile dont le pointeur de retour de fonction, ce qui provoquerait une exécution de code arbitraire.

Le correctif utilise la fonction `RSA_size()` pour déterminer la quantité de mémoire à allouer pour contenir les données chiffrées et utilise de la mémoire allouée dans le tas pour stocker ces données.

Recommandations

Il est recommandé de vérifier la version de ntp installé sur le système et d'appliquer le correctif de sécurité ou d'installer une version égale ou supérieure à la 4.2.8, qui corrige ces vulnérabilités.

Documentation

- Entrée de blog de l'équipe Google Security :
  http://googleprojectzero.blogspot.fr/
- Correctif :
  https://security.freebsd.org/patches/SA-14:31/ntp.patch
- NTP 4.2.8 :
  http://www.eecis.udel.edu/ ntp/ntp_spool/ntp4/ntp-4.2/ntp-4.2.8.tar.gz
- Bulletin de sécurité NTP :
  http://support.ntp.org/bin/view/Main/SecurityNoticeRecent_Vulnerabilities
- Avis CERTFR-2014-AVI-537 du 22 décembre 2014 :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-537/
- Avis CERTFR-2014-AVI-538 du 23 décembre 2014 :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-538/
- Avis CERTFR-2014-AVI-539 du 23 décembre 2014 :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-539/

2 - Mise à disposition d'un accès à Internet

Internet est désormais un outil de productivité incontournable. Pour répondre à ce besoin grandissant de mobilité de leurs clients ou leurs usagers, les entreprises, collectivités locales et administrations ont généralisé les points d'accès sans fil en s'appuyant sur la technologie WiFi.

Cependant, des obligations légales pèsent sur les entités qui mettent à disposition ce type d'accès. Dans un article récent, la Commission Nationale de l'Informatique et des Libertés rappelle les obligations imposées aux fournisseurs de ces services par le Code des postes et des communications électroniques.

Elles doivent tout d'abord conserver les "données de trafic" pendant un an, à compter de leur enregistrement. Il s'agit des données utiles pour rechercher, constater et poursuivre des infractions pénales. Les informations relatives aux contenus échangés (exemple : corps d'un mail, d'une page web...) ne doivent pas être conservées.

Les utilisateurs doivent également être informés des modalités de traitement de leurs données par l'organisme. Enfin, les outils de surveillance ne doivent s'appuyer que sur les données nécessaires à la supervision, sans capitaliser de données inutiles à la réalisation de cette mission.

Lors du déploiement d'un service de libre accès à Internet, l'établissement doit également s'assurer de la sécurité et de la confidentialité des données échangées sur son réseau.

Les communications sans fil doivent s'appuyer sur une protection cryptographique suffisante (exemple : WPA2). Les normes trop vulnérables doivent être prohibées (exemple : WEP). De même, des mécanismes d'authentification adaptés à la configuration du réseau sans fil doivent être utilisés. La puissance du signal émis doit permettre de couvrir une zone restreinte et contrôlée pour éviter toute capture sauvage du trafic. La connexion sur un réseau en accès libre constitue un point d'entrée dans un réseau professionnel. En conséquence, les données sensibles de l'entreprise ne devront pas être accessibles depuis cette connexion.

Des mesures particulières doivent également être prises afin de durcir les différents points d'accès. Il peut s'agir d'interdire l'accès physique au périphérique ou plus simplement de bloquer les points d'entrée (exemple : ports USB). La sécurisation s'appuie également sur une bonne administration des éléments logiciels. Ainsi, Les microcodes, systèmes d'exploitation et applications Web devront être régulièrement mis à jour. Les mots de passe d'administration devront être changés régulièrement et être suffisamment complexes. Les services non indispensables (exemple : WiFi Protected Setup) ou peu sécurisés devront être désactivés s'ils ne sont pas utilisés.

Finalement, il convient d'assurer la conservation des données techniques utiles en cas d'incident ou pour répondre à une demande d'identification émanant des autorités judiciaires. Des solutions de stockage sécurisé permettant de garantir l'intégrité des données devront être déployées.

Documentation

- ANSSI - Note Technique - Recommandations de sécurité relatives aux réseaux WiFi : http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf
- CNIL - Internet et WiFi en libre accès, bilan des contrôles : http://www.cnil.fr/linstitution/actualite/article/article/internet-et-wi-fi-en-libre-acces-bilan-des-controles-de-la-cnil/
- CNIL - Conservation des données de trafic, hot-spot, WiFi, cybercafés, employeurs, quelles obligations ? : http://www.cnil.fr/linstitution/actualite/article/article/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations/
- ANSSI - Note d'information : http://cert.ssi.gouv.fr/site/CERTA-2002-REC-002

3 - Recrudescence de courriels piégés avec document Office contenant des macros malveillantes

Microsoft indique cette semaine [1] avoir détecté au mois de décembre 2014 une forte augmentation d'envois de courriels contenant des documents Office piégés [2].

Ce type de menace avait fortement diminué depuis que la configuration par défaut des applications de la suite Office demande l'accord de l'utilisateur avant d'exécuter une macro. Néanmoins, une vague de courriels récents utilise des techniques d'ingénierie sociale pour inciter les destinataires à activer les macros. Ainsi, certains documents malveillants détaillent les étapes permettant cette activation, en imitant la charte graphique de la suite Office pour tromper l'utilisateur. D'autres documents sont laissés intentionnellement vides pour laisser penser que l'exécution d'une macro est nécessaire pour voir le contenu.

Le CERT-FR rappelle qu'il convient d'être attentif lors de la consultation d'un courriel, en particulier lorsqu'il contient une pièce jointe [3]. Aussi, il peut être judicieux de vérifier les paramètres d'exécution des macros dans la configuration des applications de la suite Office et, en cas de doute, de le faire avant d'ouvrir un document dont

la provenance n'est pas sûre [4] [5]. Une politique de sécurité interdisant la modification de ces paramètres ainsi qu'une politique de signature des macros peuvent également être mises en oeuvre.

Le CERT-FR rappelle à cette occasion que Microsoft Office 2003 n'est plus supporté depuis le 8 avril 2014.

Documentation

1 Microsoft - Alerte sur une recrudescence de courriels piégés :
https://threatpost.com/microsoft-reports-massive-increase-in-macros-enabled-threats/110204

2 Microsoft Malware Protection Center - "Avant d'activer les macros..." :
http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

3 ANSSI - Note d'information - Mesures de prévention relatives à la messagerie :
http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

4 Microsoft - Activer ou désactiver les macros - Office 2007 :
https://support.office.com/fr-fr/article/Activer-ou-d%C3%A9sactiver-les-macrosdans-les-documents-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12

5 Microsoft - Activer ou désactiver les macros - Office 2010 / Office 2013 :
https://support.office.com/fr-fr/article/Activer-ou-d%C3%A9sactiver-les-macrosdans-les-fichiers-Office-12b036fd-d140-4e74-b45e-16fed1a7e5c6

4 - Rappel des avis émis

Dans la période du 05 au 11 janvier 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-003 : Vulnérabilité dans F5 BIG-IP ASM
- CERTFR-2015-AVI-004 : Multiples vulnérabilités dans IBM Infosphere BigInsights
- CERTFR-2015-AVI-005 : Vulnérabilité dans strongSwan
- CERTFR-2015-AVI-006 : Vulnérabilité dans IBM Security Network Protection
- CERTFR-2015-AVI-007 : Multiples vulnérabilités dans EMC Documentum Web Development Kit
- CERTFR-2015-AVI-008 : Multiples vulnérabilités dans OpenSSL
- CERTFR-2015-AVI-009 : Multiples vulnérabilités dans Wireshark

Gestion détaillée du document

12 janvier 2015 version initiale.