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 22 juin 2015
N° CERTFR-2015-ACT-025

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-025

1 - Vulnérabilité Logjam

Le mercredi 20 mai 2015, un groupe de chercheurs a publié une analyse concernant l'algorithme d'échange de clés Diffie-Hellman, exposant une vulnérabilité appelée Logjam et identifiée par la référence CVE-2015-4000. Cet algorithme est utilisé dans de nombreux protocoles tels que SSH, IPsec, HTTPS et plus généralement les protocoles basés sur TLS.

Pour démarrer une connexion TLS, le client (par exemple un navigateur) et le serveur ont besoin d'échanger en toute sécurité une clé secrète. Cet échange est réalisé au cours de la « poignée de main » de TLS. Il existe différents algorithmes d'échange de clés, tel que RSA statique et Diffie-Hellman.

Logjam est similaire à la précédente vulnérabilité « Freak », impactant RSA. Ces deux vulnérabilités permettent de forcer, lors de l'établissement d'une session, l'utilisation d'un algorithme reposant sur des paramètres faibles. En effet, dans les années 90, pour pouvoir exporter de la technologie embarquant de la cryptographie en dehors des États-Unis, une loi obligeait les entreprises à utiliser des clés de taille faible. Ces options historiques sont encore présentes pour assurer une compatibilité avec d'anciens systèmes.

La vulnérabilité FREAK repose sur la fonction export de RSA, tandis que la vulnérabilité sur Logjam porte sur la fonction DHE_EXPORT de Diffie-Hellman Key Exchange (DHE).

Ainsi, tout serveur acceptant l'option DHE_Export est vulnérable. En effet, un attaquant en situation de « singe intercepteur » pourrait exploiter la vulnérabilité afin de forcer l'utilisation d'une taille de clé de 512 bits.

Un grand nombre de logiciels utilise des paramètres prédéfinis. Avec la connaissance de ces derniers, un attaquant pourrait réaliser le calcul du logarithme discret en avance de phase pour être ensuite capable de calculer la clé en quelques minutes lors de l'interception du trafic de la victime.

Un navigateur est vulnérable s'il accepte des paramètres faibles pour initialiser l'échange de clés via Diffie-Hellman. Des mises à jours sont prévues par les principaux navigateurs pour n'accepter que des paramètres supérieurs à 1024 bits. Le lien suivant permet de tester si un navigateur est vulnérable [1].

Un guide a également été publié par l'équipe de chercheurs pour aider les administrateurs à configurer leurs serveurs [2]. Une mise à jour pour OpenSSL est disponible pour forcer l'utilisation de paramètres avec un minimum de 768 bits. L'option DHE_export y est également désactivée. Une prochaine version permettra d'augmenter les paramètres requis à 1024 bits [3].

Le CERT-FR recommande donc de mettre à jour les logiciels concernés.

Documentation

1 https://weakdh.org
2 https://weakdh.org/sysadmin.html
3 https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/

2 - Détection des attaques Kerberos

Kerberos est un protocole d'authentification réseau utilisé, en particulier, en environnement Active directory. Il repose sur un mécanisme de clés secrètes, de chiffrement symétrique et sur l'utilisation de tickets.

Il existe trois acteurs dans un scénario d'authentification via Kerberos [2] :

- le client, qui souhaite s'authentifier auprès d'un serveur ;
- le serveur, qui doit s'assurer de l'authenticité du client ;
- un tiers de confiance, le KDC qui héberge un service de délivrance de ticket Kerberos.

Pour les utilisateurs, chaque acteur possède un ensemble de clés dérivées de leur mot de passe. Pour le secret du service de délivrance de ticket Kerberos, Active Directory utilise un compte utilisateur dénommé `krbtgt`. Il s'agit d'un compte d'infrastructure, toujours désactivé et sans droit (au sens permission dans l'Active Directory) ni privilège particulier.

Les étapes simplifiées des différents échanges lors de l'authentification d'un utilisateur auprès d'un service (exemple le service CIFS sur le serveur SERV01) sont :

1. `KRB_AS_REQ` : l'utilisateur demande un ticket d'authentification (TGT). Pour prouver qu'il connait la clé utilisateur, il envoie au KDC un horodatage chiffré à l'aide de sa clé (cette étape est appelée la pré-authentification).
2. `KRB_AS_REP` : le KDC vérifie le compte utilisateur et valide la clé utilisée pour la pré-authentification. Il renvoie alors un TGT chiffré à l'aide de sa clé (dérivée du mot de passe du compte `krbtgt`). Ce ticket contient les informations d'autorisation de l'utilisateur (PAC).
3. `KRB_TGS_REQ` : lorsque l'utilisateur souhaite accéder à un service, il effectue une demande au KDC de ticket de service TGS (par exemple pour le service CIFS hébergé sur le serveur SERV1) à laquelle il joint le TGT précédemment obtenu.
4. `KRB_TGS_REP` : le KDC valide la demande en déchiffrant le TGT et vérifie le code de contrôle/checksum de la PAC. Si celui-ci est valide, il renvoie un ticket de service TGS chiffré à l'aide de la clé du service cible.
5. `KRB_AP_REQ` : l'utilisateur se connecte alors au serveur hébergeant le service en présentant son TGS.
6. `KRB_AP_REP` : le service déchiffre le TGS et, si la validation du PAC n'est pas demandée, aucune vérification sur authenticité de l'utilisateur n'est effectuée auprès du contrôleur de domaine.

Plusieurs attaques reposant sur la construction de ces messages sont possibles, notamment selon les données dont dispose l'attaquant.

Golden Ticket

Si un attaquant dispose de la clé du compte `krbtgt` (par exemple lors d'un export de la base de compte d'un contrôleur de domaine), il peut forger un ticket d'authentification (TGT) pour n'importe quel utilisateur, même inexistant. Il peut également forger un ticket TGT malveillant en ajoutant à la PAC des SID de groupe auxquels l'utilisateur n'appartient pas. L'attaquant est ensuite en mesure de forger des demandes de TGS (KRB_TGS_REQ) en utilisant ce TGT.

Ces attaques sont possibles, car, lors de la validation par le contrôleur de domaine de la demande de ticket de service, cette requête de TGS est considérée comme légitime. Un ticket de service TGS est alors généré à partir d'informations sous le contrôle de l'attaquant. De plus, le contrôleur de domaine ne vérifie la validité du compte utilisateur que si le ticket dépasse une limite de temps (la valeur par défaut est de 20 minutes).

Silver Ticket

Si l'attaquant dispose de la clé d'un service, il peut alors forger directement un ticket de service. Ce ticket ne pourra être utilisé que pour ce service spécifique limitant le périmètre de l'attaque. Par exemple, l'attaquant pourra dès lors modifier son accès à ce service (par exemple en forgeant une PAC qui sera aveuglément acceptée par le serveur cible). Contrairement au scénario du Golden ticket, aucune interaction n'est effectuée avec le contrôleur de domaine, rendant l'attaque plus furtive et sa détection plus fastidieuse.

La détection de ces attaques est difficile. Aujourd'hui, elle est généralement réalisée au moyen des journaux de sécurité et donc son efficacité dépend directement de la qualité des évènements enregistrés [4]. Une attention particulière doit être portée aux évènements suivants :

- Sur les systèmes :
  - Evènements ID 4624 (Account Logon) : l'ouverture de session d'un compte s'est correctement déroulée.

  - Evènements ID 4672 (Admin Logon) : privilèges spéciaux assignés à la nouvelle session.
- Sur les contrôleurs de domaine :
  - Evènements ID 4769 (Kerberos TGS Request) : un ticket de service Kerberos a été demandé.
  - Evènements ID 4768 (Kerberos TGT Request): un ticket d'authentification Kerberos (TGT) a été demandé.

Un volume important de tickets légitimes est généré chaque jour. Il est difficile de faire émerger ceux de l'attaquant. Un des moyens de les détecter est d'identifier des anomalies dans les évènements enregistrés dans les journaux [1].

Ainsi, lors de l'authentification d'un utilisateur, les évènements d'ouverture et fermeture de session (EventID 4624 et 4634) contiennent les champs suivants :

```
Security ID: DOMAIN\AccountID
Account Name: AccountID
Account Domain: DOMAIN (nom netbios)
```

Exemple :

```
Security ID: TESTLAB\Administrateur
Account Name: Administrateur
Account Domain: TESTLAB
```

Il a été remarqué que les outils disponibles permettant de forger des tickets à titre éducatif intègrent aux champs des évènements générant des éléments permettant de les différencier (voir le tableau ci-dessous).

	Golden ticket standard	**Golden ticket Pykek (MS14-068)**	**Golden ticket Kekeo(MS14-068)**	**Silver Ticket**
Account Logon Evt ID 4624	Account Domain: "FQDN" au lieu de "domain"	Account Name != Security ID Account Domain: "FQDN"	Account Domain: "FQDN" au lieu de "domain"	Account Domain: <NULL> au lieu de "domain"
Account Logoff Evt ID 4634				Account Domain: <NULL> au lieu de "domain"
Admin Logon Evt ID 4672	Account Domain: <NULL> au lieu de "domain"	Account Name != Security ID Account Domain: "FQDN"	Account Domain: <NULL> au lieu de "domain"	Account Domain: <NULL> au lieu de "domain"
TGS-REQ Evt ID 4769		Account Domain: "FQDN" au lieu de "domain"	Account Domain: "FQDN" au lieu de "domain"	

Le CERT-FR attire l'attention sur les limites de cette méthode qui ne peut être totalement efficace puisqu'il suffit à un attaquant déterminé de forger des tickets ne présentant pas les caractéristiques évoquées ci-dessus. Pour une analyse en profondeur, une politique cohérente de journalisation et de centralisation doit être mise en place sur les contrôleurs de domaine, mais aussi sur l'ensemble des machines du domaine. La mise en corrélation alors possible des évènements d'ouverture de session (4624) conjointement aux évènements indiquant un changement de privilège (4672) peut alors permettre la détection d'anomalies dans le déroulement de la session.

Récemment de nombreux outils reposant sur l'analyse de chemins de contrôle ont vu le jour (AD-Control-Paths [5] et Aorato la solution Microsoft). Ils offrent une réponse prometteuse à la recherche de comportement déviant en environnement Active Directory.

Documentation

1 Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory)
http://adsecurity.org/?p=1515

2 Secrets d'authentification épisode II Kerberos contre-attaque
https://www.sstic.org/media/SSTIC2014/SSTIC-actes/secrets_dauthentification_pisode_ii__kerberos_cont/SSTIC2014-Article-secrets_dauthentification_pisode_ii__kerberos_contre-attaque-bordes_2.pdf

3 Kerberos Vulnerability in MS14-068 (KB3011780) Explained
http://adsecurity.org/?p=541

4 WINDOWS LOGGING CHEAT SHEET
http://static1.1.sqspcdn.com/static/f/1777801/26121061/1429301073300/Windows+Logging+Cheat+Sheet+v1.1.pdf

5 https://github.com/ANSSI-FR/AD-control-paths

3 - Rappel des avis émis

Dans la période du 15 au 20 juin 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-258 : Vulnérabilité dans Huawei E5756s
- CERTFR-2015-AVI-259 : Multiples vulnérabilités dans les produits BlueCoat
- CERTFR-2015-AVI-260 : Multiples vulnérabilités dans Drupal
- CERTFR-2015-INF-001 : DNS Rebinding

Gestion détaillée du document

22 juin 2015 version initiale.