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 17 octobre 2014
N° CERTFR-2014-ACT-042

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-042

1 - Changement de jour pour la publication du bulletin d'actualité

À partir de la semaine prochaine, le bulletin d'actualité du CERT-FR ne sera plus publié le vendredi soir mais le lundi matin.

En conséquence, la date de publication du prochain bulletin d'actualité est le 27 octobre 2014.

2 - Vulnérabilité concernant SSLv3

Description de la vulnérabilité

Le 14 octobre 2014, Google a rendu publique l'existence d'une attaque sur le protocole SSL 3.0. Cette attaque, surnommée «Poodle», exploite une faiblesse de ce protocole et non une erreur d'implémentation. Tous les systèmes susceptibles d'établir des connexions sécurisées en SSL 3.0 sont donc concernés. Cependant, les évolutions du protocole SSL, à savoir TLS, ne sont pas impactées. L'alerte CERTFR-2014-ALE-007 a été publiée pour informer des risques liés à cette attaque.

L'exploitation de cette vulnérabilité par une personne malveillante peut permettre d'accéder en clair à des données protégées par le protocole SSL. En particulier, cette attaque peut exposer des utilisateurs à des vols de témoins de connexion («cookies») utilisés par les navigateurs pour stocker des identifiants de session.

Pour mettre en œuvre l'attaque, il est nécessaire de pouvoir :

– injecter ses propres données avant et après la valeur secrète recherchée ;
– intercepter et modifier le trafic réseau.

Le scénario le plus probable qui vérifie ces deux pré-requis serait celui d'un faux point d'accès Wi-Fi sous le contrôle d'une personne malveillante et qui permettrait d'injecter du code JavaScript exécuté par le navigateur de la victime pour réaliser l'attaque. De plus, l'attaquant doit pouvoir provoquer des erreurs de connexion au niveau réseau pour forcer le navigateur de la victime à basculer de TLS vers SSL 3.0.

Recommandations

La recommandation prioritaire est de désactiver le support du protocole SSL 3.0 au niveau des navigateurs Internet. L'alerte CERTFR-2014-ALE-007 précise les changements de configuration à réaliser sur Internet Explorer et Firefox qui permettent cette désactivation. Dans un second temps, il est également recommandé de désactiver le support de SSL 3.0 au niveau des serveurs. Cependant, il convient de qualifier ce changement en amont car il peut empêcher certains clients qui ne supporteraient que SSL 3.0 de se connecter.

Documentation

– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-007
– http://googleonlinesecurity.blogspot.ie/2014/10/this-poodle-bites-exploiting-ssl-30.html

3 - Collecte de données par la version d'évaluation de Windows 10

Depuis le 01 octobre 2014, Microsoft met à disposition une version d'évaluation de son prochain système d'exploitation Windows 10.

Lors de l'utilisation de cette version préliminaire ayant pour objet l'évaluation de fonctionnalités (Technical Preview), de nombreuses données sont collectées et transmises automatiquement à Microsoft. Elles peuvent alors être combinées à des informations liées à votre compte Microsoft. De plus, certaines informations peuvent être partagées avec des partenaires de Microsoft.

La déclaration de confidentialité liste des données collectées et les moyens utilisés.

Informations collectées :

- les appareils utilisés ;
- l'adresse IP, l'état du réseau et ses conditions d'exploitation ;
- les logiciels exécutés, des informations sur les fichiers, les applications utilisées pour les ouvrir et les temps d'ouverture ;
- les fonctionnalités les plus souvent utilisées et leur fréquence ;
- les caractères tapés, les informations vocales ;
- les performances, la fiabilité, la réactivité (lors du clic sur un bouton par exemple), les problèmes rencontrés ;
- les préférences et paramètres de l'utilisateur.

Moyens de collecte :

- dons volontaires des données par l'utilisateur, à l'occasion de l'inscription à un service ou d'une demande de support ;
- récolte automatique par le système lors de son installation et de son utilisation ;
- techniques classiques telles que les cookies et fonctionnalités similaires.

La déclaration de confidentialité précise qu'il n'est pas possible de désactiver complètement la transmission de ces données.

Le CERT-FR recommande donc de ne pas utiliser cette version d'évaluation de Windows 10 pour traiter et stocker des informations sensibles. Plus généralement, pour rappel, une version d'évaluation d'un logiciel ne doit pas être utilisée au sein d'un système d'information de production.

Documentation

- Déclaration de confidentialité de Microsoft :
  http://windows.microsoft.com/fr-fr/windows/preview-privacy-statement

4 - Mise à jour mensuelle de Microsoft

Le 14 octobre 2014, lors de sa mise à jour mensuelle, Microsoft a publié huit bulletins de sécurité dont trois considérés comme critiques et cinq comme importants :

- MS14-056 (critique) qui concerne Internet Explorer ;
- MS14-057 (critique) qui concerne .NET ;
- MS14-058 (critique) qui concerne le noyau de Windows ;
- MS14-059 (important) qui concerne ASP .NET MVC ;
- MS14-060 (important) qui concerne la gestion des objets OLE dans Windows (Office) ;
- MS14-061 (important) qui concerne Microsoft Word et Office Web Apps ;
- MS14-062 (important) qui concerne le service de messages de Windows ;
- MS14-063 (important) qui concerne le pilote pour les partitions FAT32 de Windows.

Dans cette mise à jour, quatorze vulnérabilités sont corrigées dans Internet Explorer. La plupart d'entre elles sont des corruptions de mémoires susceptibles de conduire à l'exécution de code arbitraire à distance. Les autres permettent une élévation de privilèges ou un contournement de la distribution aléatoire de l'espace d'adressage (ASLR).

La vulnérabilité corrigée dans .NET peut conduire à un déni de service pour un site Internet basé sur .NET si des requêtes spécifiques contenant des caractères internationaux lui sont soumises. Cette vulnérabilité est particulièrement critique sous .NET 4.5 car la fonctionnalité vulnérable (*iriParsing*) est activée par défaut et ne peut être désactivée (contrairement à .NET 4.0).

Concernant le noyau Windows, deux vulnérabilités sont corrigées. Elles peuvent conduire à une exécution de code arbitraire à distance si un utilisateur ouvre un document ou visite un site Web contenant des polices TrueType exploitant ces vulnérabilités.

De même, la vulnérabilité corrigée dans ASP .NET MVC permet de contourner la politique de sécurité si l'utilisateur visite un site Web malveillant.

La vulnérabilité concernant Windows OLE peut amener à une exécution de code arbitraire à distance. Pour cela, l'utilisateur doit ouvrir un document Microsoft Office contenant un objet OLE conçu pour exploiter cette vulnérabilité.

Au niveau de Microsoft Word et Microsoft Office Web Apps, une vulnérabilité permettant l'exécution de code à distance est corrigée. Son exploitation nécessite qu'un utilisateur ouvre un document Word conçu pour exploiter cette vulnérabilité.

Le service *Message Queuing* de Microsoft Windows présente une vulnérabilité pouvant conduire à une élévation de privilèges. Son exploitation passe par l'envoi d'une requête de contrôle d'entrée/sortie (IOCTL) spécifique à ce service et permet une prise de contrôle complète du système. Néanmoins, ce service n'est pas installé par défaut et nécessite les droits d'administration pour l'installer.

Enfin, la vulnérabilité corrigée dans le pilote de partition de disque FAT32 permet une élévation de privilèges. Elle se situe au niveau de la sous-attribution de la mémoire tampon et permet d'écrire des données dans des parties du système d'exploitation qui sont normalement réservées.

Le CERT-FR souhaite insister sur l'importance de certains de ces bulletins (MS14-058 et MS14-060). En effet, l'exploitation des vulnérabilités corrigées par ces bulletins a pu être observée dans le cadre d'attaques sur des systèmes d'information.

Ainsi, le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Documentation

- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-417/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-418/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-419/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-420/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-421/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-422/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-423/
- http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-424/

5 - Rappel des avis émis

Dans la période du 10 au 16 octobre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-007 : Vulnérabilité dans SSLv3
- CERTFR-2014-ALE-008 : Vulnérabilité dans Drupal
- CERTFR-2014-AVI-413 : Multiples vulnérabilités dans le noyau Ubuntu
- CERTFR-2014-AVI-414 : Vulnérabilité dans Huawei E355
- CERTFR-2014-AVI-415 : Multiples vulnérabilités dans les systèmes SCADA Siemens
- CERTFR-2014-AVI-416 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2014-AVI-417 : Vulnérabilité dans le pilote FAT32 de Microsoft Windows
- CERTFR-2014-AVI-418 : Vulnérabilité dans le service Message Queuing de Microsoft Windows
- CERTFR-2014-AVI-419 : Vulnérabilité dans Microsoft Word et Microsoft Office Web Apps
- CERTFR-2014-AVI-420 : Vulnérabilité dans Microsoft Windows OLE
- CERTFR-2014-AVI-421 : Vulnérabilité dans Microsoft ASP.NET MVC
- CERTFR-2014-AVI-422 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2014-AVI-423 : Multiples vulnérabilités dans Microsoft .NET Framework
- CERTFR-2014-AVI-424 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-425 : Multiples vulnérabilités dans la suite de produits Sun de Oracle

- CERTFR-2014-AVI-426 : Multiples vulnérabilités dans les solutions de virtualisation d'Oracle
- CERTFR-2014-AVI-427 : Multiples vulnérabilités dans Oracle MySQL
- CERTFR-2014-AVI-428 : Multiples vulnérabilités dans Oracle Database Server
- CERTFR-2014-AVI-429 : Multiples vulnérabilités dans Oracle Java SE
- CERTFR-2014-AVI-430 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTFR-2014-AVI-431 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-432 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2014-AVI-433 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2014-AVI-434 : Vulnérabilité dans Drupal
- CERTFR-2014-AVI-435 : Multiples vulnérabilités dans OpenSSL

Gestion détaillée du document

17 octobre 2014 version initiale.