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 07 février 2014
N° CERTFR-2014-ACT-006

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-006

1 - Mises à jour Firefox et TLS 1.2

La version 27 de Firefox est disponible depuis le 4 février. Elle corrige 13 vulnérabilités dont 4 présentées comme critiques. Le débogueur JavaScript dispose désormais d'une fonctionnalité permettant de décoder un code brouillé (obfuscation), ce qui peut être particulièrement utile pour l'analyse de code potentiellement malveillant.

Cette version comprend également une évolution importante en matière de sécurité. En effet, les protocoles TLS 1.1 et TLS 1.2 permettant de sécuriser les communications sont désormais activés par défaut.

TLS : Historique

SSL/TLS est un protocole réseau très répandu s'insérant entre la couche transport (TCP) et la couche applicative (HTTP, SMTP, IMAP, etc.) pour garantir certaines propriétés de sécurité :

- authentification du serveur (et éventuellement du client) ;
- confidentialité des données échangées ;
- intégrité des données échangées.

SSL (*Secure Socket Layer*) et TLS (*Transport Layer Security*) désignent en pratique le même protocole qui a évolué dans le temps. À l'origine, SSLv2 a été publié en 1995 par Netscape pour permettre la mise en œuvre d'échanges sécurisés sur Internet : HTTPS était né. Cependant, de nombreuses failles structurelles présentes dans SSLv2 ont très vite mené à SSLv3 en 1996.

Au début des années 2000, le protocole a subi quelques améliorations pour devenir TLS 1.0. A partir de cette version, c'est l'IETF qui a pris en charge la maintenance du protocole (la RFC 2246 définissant TLS 1.0 a été publiée en 2001). Depuis, le protocole a connu deux nouvelles versions : TLS 1.1 (RFC 4346 en 2006) et TLS 1.2 (RFC 5246 en 2008).

L'usage le plus répandu de TLS aujourd'hui est celui qui en est fait par le protocole HTTPS, c'est-à-dire l'encapsulation du protocole réseau HTTP pour apporter les propriétés de sécurité. TLS connaît également d'autres usages : les protocoles de messagerie électronique (SMTP, POP, IMAP), certaines implémentations de réseaux privés virtuels (VPN) ou encore l'authentification EAP-TLS qui peut être mise enœuvre dans certains réseaux Wifi WPA2.

Début 2014, SSLv2 n'est quasiment plus utilisé sur Internet. Les versions du protocole que l'on rencontre le plus souvent en pratique sont TLS 1.0 et SSLv3. En effet, le déploiement des versions plus récentes a été très lent jusque récemment. Depuis quelques années, de nombreuses attaques ont été publiées sur le protocole TLS, mettant en évidence le besoin de migrer vers les versions 1.1 et 1.2.

TLS 1.1 et 1.2

TLS 1.1 apporte une contremesure fiable à l'attaque `BEAST`, décrite par Rizzo et Duong en 2011. TLS 1.2 permet théoriquement de contrer une large gamme d'attaques (`BEAST`, mais aussi `Lucky13` et les vulnérabilités liées à RC4) car cette dernière version offre une plus grande agilité cryptographique : un client et un serveur supportant

le protocole TLS 1.2 peuvent négocier des algorithmes cryptographiques récents (AES en mode GCM) offrant de meilleures propriétés que les algorithmes historiques. Du point de vue de HTTPS, la majorité des serveurs est aujourd'hui théoriquement capable de répondre en TLS 1.2, même si cette version du protocole n'est pas toujours activée par défaut.

Documentation

- Bulletin d'actualité CERTA-2011-ACT-039 sur la vulnérabilité `BEAST` :
  http://www.cert.ssi.gouv.fr/site/CERTA-2011-ACT-039
- Bulletin d'actualité CERTA-2013-ACT-009 sur la vulnérabilité `Lucky13` :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-009

2 - Correction d'une vulnérabilité critique visant le lecteur Flash d'Adobe

Le 04 février 2014, *Adobe* a publié un correctif de sécurité visant son produit *Flash Player*. Cette mise à jour corrige la vulnérabilité CVE-2014-0497 qui permet une exécution de code arbitraire à distance. Découverte par *Kaspersky Labs*, la faille semble être exploitée par des groupes d'attaquants.

Cette mise à jour a été mise à disposition par Adobe en dehors de son cycle habituel de fourniture de correctifs ce qui témoigne de l'importance des risques liés à cette vulnérabilité.

Le CERT-FR recommande donc l'application de cette mise à jour dès que possible.

Documentation

- Bulletin de sécurité CERTFR-2014-AVI-052 du 04 février 2014 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-052/
- Bulletin d'actualité Adobe APSB14-04 du 04 février 2014 :
  http://helpx.adobe.com/security/products/flash-player/apsb14-04.html

3 - Rappel des avis émis

Dans la période du 31 janvier au 06 février 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-048 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-049 : Vulnérabilité dans Puppet
- CERTFR-2014-AVI-050 : Vulnérabilité dans Citrix XenMobile
- CERTFR-2014-AVI-051 : Vulnérabilité dans F5 BIG-IP
- CERTFR-2014-AVI-052 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2014-AVI-053 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2014-AVI-054 : Vulnérabilité dans EMC Documentum Foundation Services

Gestion détaillée du document

07 février 2014 version initiale.