Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 19 octobre 2012
N° CERTA-2012-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-042

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-042`

1 Correctifs Oracle

Oracle a publié cette semaine des mises à jours corrigeant plus d'une centaine de vulnérabilités dans de nombreux produits comme *MySQL*, *Java*, *Oracle Database 11g*, *People Soft*, *Virtual Box*, etc.
La vulnérabilité la plus critique porte la référence « CVE-2012-3137 » et fait l'objet d'un article spécifique de ce bulletin d'actualité.

Il est important de noter que de nombreuses solutions tiers utilisent des composants *Oracle*. Des mises à jour de ces solutions sont à prévoir.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Bulletin de sécurité Oracle du 16 Octobre 2012 :
  http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
- Bulletin de sécurité Oracle Java du 16 Octobre 2012 :
  http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html

2 Retour sur une vulnérabilité TLS récente : CRIME

2.1 Contexte

Lors de la conférence Ekoparty de septembre 2012, les chercheurs Juliano Rizzo (Netifera) et Thai Duong (Google) ont présenté une attaque pratique visant le protocole TLS et plus particulièrement HTTPS et SPDY (qui utilisent TSL comme couche de sécurité), un protocole proche de HTTP focalisé sur les performances. Comme l'attaque BEAST présentée par les mêmes chercheurs en 2011 (cf. CERTA-2011-ACT-039), CRIME a largement été médiatisée. Elle permet une nouvelle fois à un attaquant, sous certaines conditions, de récupérer les *cookies* de session d'un site protégé par TLS. Ce *cookie* permet alors à l'attaquant de se faire passer pour la victime sur le site visé.

2.2 Principe

L'attaque est basée sur les problèmes liés à l'utilisation combinée de la compression et du chiffrement. Afin de réaliser l'attaque, l'attaquant doit pouvoir manipuler une partie des données qui seront ensuite compressées et

chiffrées. Il doit également pouvoir observer le trafic chiffré résultant. Par exemple, soit `données = entrée + secret`, ensuite compressées et chiffrées : `chiffré = chiffrement(compression(données))`.

Si l'attaquant contrôle `entrée` et peut observer la longueur de `chiffré`. Alors, compte tenu du fonctionnement des algorithmes de compression, qui utilisent la redondance de l'information pour optimiser l'espace utilisé, l'attaquant peut moduler `entrée` afin de déterminer tout ou partie de `secret`.

En effet, pour une `entrée` de taille donnée, la longueur de `chiffré` sera inférieure si `entrée` contient des données également présentes dans `secret`.

2.3 Application pratique

En théorie, l'application de la vulnérabilité ne se limite pas aux protocoles HTTPS et SPDY, pris comme exemples lors de la présentation.

En pratique, HTTPS et SPDY sont plus particulièrement vulnérables, car le secret est ici le *cookie* de session de la victime. Si un attaquant peut réaliser des requêtes vers des URL arbitraires sur le serveur visé et observer le trafic, alors il peut mettre en œuvre l'attaque décrite.

Or, si l'attaquant peut modifier le trafic par une attaque de l'homme du milieu, les conditions sont remplies dès lors que la victime navigue à la fois sur le site sécurisé et sur un site en HTTP.

L'attaquant peut en effet injecter du code, par exemple javascript, dans la page en HTTP qui effectuera des requêtes de son choix vers le site HTTPS. Pouvant injecter du trafic, il peut également observer les requêtes chiffrées et donc décrypter les *cookies* de session en quelques minutes.

Par exemple, un tel scénario est relativement simple à mettre en œuvre sur un réseau Wifi ouvert.

2.4 Logiciels vulnérables

Les deux navigateurs affectés par cette attaque sur les *cookies* sont Mozilla Firefox et Google Chrome, qui sont les seuls à implémenter la compression TLS et SPDY. Cependant, d'autres logiciels utilisant TLS peuvent être concernés par des vulnérabilités similaires. Notamment, les navigateurs qui utilisent la compression HTTP gzip.

2.5 Mesures de protection

Mozilla (CERTA-2012-AVI-561) et Google (CERTA-2012-AVI-476) ont mis à jour leurs navigateurs pour corriger la vulnérabilité. Le CERTA recommande donc d'installer les dernières versions de ces logiciels afin de se protéger.

Documentation

- Support de la présentation de CRIME à Ekoparty
  https://docs.google.com/presentation/d/11eBmGiHbYcHR9gL5nDyZChu_-lCa2GizeuOfaLU2HOU/edit
- Bulletin d'actualité CERTA-2011-ACT-039 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-039/
- Avis CERTA-2012-AVI-561 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-561/
- Avis CERTA-2012-AVI-476 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-476/
- Référence CVE-2012-4929 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4929
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4929
- Référence CVE-2012-4930 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4930
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4930

3 Problématique du mot de passe unique

Pour s'authentifier sur divers espaces privés et publics tels qu'une boîte de messagerie, un compte en banque, des sites de réseaux sociaux, des forums de discussions, des sites marchands, des réseaux ou applications professionnelles, l'utilisateur doit généralement fournir un nom de compte et un mot de passe valides.

Lorsqu'il crée un compte, l'utilisateur fournit un nom d'utilisateur et un mot de passe qui seront ensuite stockés dans une base de données en clair ou bien sous forme de condensat (md5, sha1, etc).

L'actualité démontre régulièrement que des sites peu sécurisés sont victimes d'attaques visant à extraire, voire à publier, la base de données de leurs utilisateurs (comprenant souvent des adresses de messagerie, identifiants, mots de passe).

Les attaquants peuvent alors, directement récupérer les mots de passe s'ils sont stockés en clair, ou en attaquer les condensats s'ils sont trop faibles, via des attaques par force brute, par dictionnaire ou grâce aux « tables arc-en-ciel » (aussi appelées *rainbow tables*). Les personnes malveillantes chercheront ensuite à s'authentifier frauduleusement et à usurper l'identité d'utilisateurs légitimes sur d'autres systèmes privés ou professionnels auxquels ils ont accès.

Pour ces raisons, il est important de choisir un mot de passe robuste et différent pour chaque site ou application utilisée. Dans le cas contraire, une compromission de la base de données de l'un de ces systèmes expose leurs utilisateurs à des accès illicites possibles à d'autres de leurs comptes, privés ou professionnels.

Le CERTA recommande de :

- sensibiliser régulièrement les utilisateurs à cette menace ;
- définir des politiques de gestion de mots de passe solides et régulièrement renouvelés (cf. documentation).

Documentation :

- Recommandations de sécurité relatives aux mots de passe :
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

4 Vulnérabilité recente sur le protocole d'authentification du SGBD Oracle

4.1 Contexte

Lors de la conférence Ekoparty de septembre 2012, le chercheur Esteban Fayo (Argeniss) a présenté un nouvelle vulnérabilité critique du protocole d'authentification de Oracle 11g, similaire à celle affectant la version 10g, publiée en avril 2012.

Ces vulnérabilités permettent à un attaquant d'obtenir, sans authentification, un condensat de mot de passe. Ce condensat peut être utilisé pour réaliser une attaque en force brute et tenter de retrouver le mot de passe en clair.

Il est important de souligner que l'attaquant n'a besoin de connaître que l'adresse IP du serveur et le SID (l'identifiant) de la base. De plus, aucune trace n'est engendrée dans les journaux. Elle n'affecte cependant que l'authentification intégrée : les authentifications externes (LDAP, Kerberos, etc.) ne sont pas concernées.

4.2 Oracle 11g

Oracle dispose d'une fonctionnalité qui permet à un utilisateur de vérifier et de changer son mot de passe en une seule opération, ce qui est particulièrement utile en cas de compte bloqué.

Une fois connecté au serveur, ce qui nécessite de connaître le SID de la base, l'attaquant obtient un aléa de 40 octets chiffré avec AES-192-CBC. La clé utilisée est un condensat du mot de passe de l'utilisateur et d'un différenciateur (graine). Or, l'aléa n'étant long que de 40 octets, 8 octets de bourrage (*padding*) sont nécessaires pour atteindre la taille de bloc requise. Le bourrage étant réalisé avec la norme PKCS#7, ces 8 octets ont pour valeur 0x08.

L'attaquant dispose donc d'un "oracle" (ou moyen de décision) qui lui permet de déterminer si un mot de passe est valide :

1. choix d'un mot de passe candidat `mdp`
2. calcul de `h = SHA1(mdp||graine)`
3. mise à la clé de AES avec la clé `h||00000000`
4. déchiffrement AES-192-CBC de l'aléa
5. vérification du padding

L'exploitation de cette vulnérabilité a été implémentée dans plusieurs outils d'attaque très répandus. Ces outils permettent aux attaquants de tester plusieurs millions de mots de passe par seconde sur une machine standard.

4.3 Oracle 10g

Une vulnérabilité similaire (cf. CERTA-2012-AVI-220) avait été publiée et corrigée en avril 2012 mais celle-ci n'était applicable qu'aux comptes bloqués. L'attaquant doit donc au préalable, dans la configuration par défaut, faire 10 tentatives d'authentification échouées pour bloquer le compte, ce qui crée une trace dans les journaux.

4.4 Se protéger

Oracle a publié cette semaine une mise à jour qui permet de se protéger de la vulnérabilité visant la version 11 (cf. CERTA-2012-AVI-577). En plus de l'application de la mise à jour, il est nécessaire de configurer l'option `SQLNET.ALLOWED_LOGON_VERSION=12`. Toutefois, l'activation de cette option peut génerer des problèmes de compatibilité avec certains clients de version inférieure.

De manière générale, et en particulier pour ces deux vulnérabilités, une protection efficace contre les attaques sur les mots de passe est d'appliquer une politique de complexité (cf. section documentation).

Le CERTA recommande donc d'appliquer les mises à jour concernées et de choisir des mots de passe robustes pour les comptes d'accès à la base de données.

Documentation

- Oracle Critical Patch Update Advisory - October 2012
  http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
- Recommandations de sécurité sur les mots de passe
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Team Shatter Advisory: OCIPasswordChange API leaks information of password hash
  https://www.teamshatter.com/?p=3434
- Avis CERTA-2012-AVI-220 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-220/
- Avis CERTA-2012-AVI-577 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-577/

5 Petit lifting du site du CERTA

Le site Web du CERTA a subi un léger lifting. Outre quelques modifications cosmétiques :

- la présentation des rubriques a été ré-agencée pour en améliorer la pertinence ;
- les résultats de la recherche de documents sont à présent ordonnés par numéros de document décroissants ;
- une rubrique « l'ANSSI recrute » a été ajoutée pour accéder notamment aux offres d'emploi du CERTA sur le site de l'ANSSI ;
- un nouveau flux RSS a été mis en place pour améliorer le suivi des avis et alertes de sécurité SCADA.

N'hésitez pas à nous faire part de vos remarques et suggestions d'amélioration par courriel adressé à : certa-svp@certa.ssi.gouv.fr.

6 Rappel des avis émis

Dans la période du 12 au 18 octobre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-564 : Multiples vulnérabilités dans Cisco ASA
- CERTA-2012-AVI-565 : Vulnérabilité dans Joomla!
- CERTA-2012-AVI-566 : Vulnérabilités dans HP Secure Web Server
- CERTA-2012-AVI-567 : Multiples vulnérabilités dans Cisco Firewall Services Module
- CERTA-2012-AVI-568 : Multiples vulnérabilités dans Cisco WebEx
- CERTA-2012-AVI-569 : Vulnérabilité dans ISC BIND
- CERTA-2012-AVI-570 : Vulnérabilité dans Symantec Ghost
- CERTA-2012-AVI-571 : Vulnérabilités dans EMC NetWorker Module
- CERTA-2012-AVI-572 : Vulnérabilités dans Google Chrome

- CERTA-2012-AVI-573 : Multiples vulnérabilités dans IBM HTTPSRV
- CERTA-2012-AVI-574 : Vulnérabilité dans le système SCADA Schneider Electric Critical Power and Cooling Services
- CERTA-2012-AVI-575 : Vulnérabilités dans le système SCADA Schneider Electric TAC I/A
- CERTA-2012-AVI-576 : Multiples vulnérabilités dans Oracle Java
- CERTA-2012-AVI-577 : Multiples vulnérabilités dans Oracle Database Server
- CERTA-2012-AVI-578 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2012-AVI-579 : Multiples vulnérabilités dans Oracle MySQL
- CERTA-2012-AVI-580 : Multiples vulnérabilités dans Oracle E-Business Suite
- CERTA-2012-AVI-581 : Multiples vulnérabilités dans Oracle Supply Chain
- CERTA-2012-AVI-582 : Multiples vulnérabilités dans Oracle People Soft
- CERTA-2012-AVI-583 : Vulnérabilités dans Oracle Siebel CRM
- CERTA-2012-AVI-584 : Vulnérabilités dans Oracle Industry Applications
- CERTA-2012-AVI-585 : Multiples vulnérabilités dans Oracle Financial Services Software
- CERTA-2012-AVI-586 : Multiples vulnérabilités dans Oracle Sun Products Suite
- CERTA-2012-AVI-587 : Vulnérabilités dans Oracle Virtualization
- CERTA-2012-AVI-588 : Vulnérabilité dans AWStats
- CERTA-2012-AVI-589 : Multiples vulnérabilités dans Java pour Apple OS X

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2012-AVI-561-001 : Multiples vulnérabilités dans les produits Mozilla (ajout de deux bulletins)

Gestion détaillée du document

19 octobre 2012 version initiale.