Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mai 2011
N° CERTA-2011-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-20

Gestion du document

Référence	CERTA-2011-ACT-020
Titre	Bulletin d'actualité 2011-20
Date de la première version	20 mai 2011
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-020.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-020/

1 Vulnérabilité dans OpenSSL

Cette semaine, deux chercheurs ont publié une attaque contre l'implémentation par OpenSSL de la signature DSA basée sur les courbes elliptiques (ECDSA), dans le cas de courbes sur un corps fini de caractéristique 2. Cette attaque repose sur la mesure du temps écoulé pour le calcul des signatures. L'analyse du temps d'exécution permet de déduire des informations sur les entrées, notamment la clef secrète. Cette classe d'attaque (*timing attacks*) a plusieurs fois conduit OpenSSL à évoluer (CVE-2003-0078, CVE-2003-0147).

En pratique, l'attaque décrite ne permet de retrouver la clef secrète que si les variations entre les mesures de temps effectuées lors de la création de différentes signatures reflètent avec une grande précision les variations entre les temps d'exécution de la multiplication d'un point de base de la courbe par un entier, opération réalisée à la production de chaque signature. Les conditions optimales sont réunies quand l'attaquant est sur l'ordinateur qui signe (serveur) et si celui-ci n'est pas trop chargé. Cette cohabitation peut résulter de l'injection d'un code malveillant aux ordres de l'attaquant sur le serveur ou de la virtualisation : l'attaquant est sur une machine virtuelle et le serveur victime sur une autre. La finesse de la mesure et l'efficacité de l'attaque décroissent rapidement si le serveur est chargé ou si l'attaquant est distant.

En attendant un correctif dans la bibliothèque OpenSSL, mais également de manière générale, il convient de s'assurer de la salubrité des serveurs utilisés pour les signatures, c'est-à-dire de l'absence de codes malveillants, et de l'hygiène informatique des machines virtuelles cohébergées.

1.1 Documentation

– Brumley, B. B., Tuveri, N. *Remote Timing Attacks are Stil Practical* :
http://eprint.iacr.org/2011/232.pdf

2 Cycle de vie des versions de Firefox

La fondation Mozilla à l'origine du navigateur `Firefox` a récemment communiqué sur la poursuite de la maintenance de la branche 3.5 de Firefox. En effet, elle indique dans un article (cf. Documentation) qu'avec l'arrivée de la version 4 et bientôt de la version 5 du navigateur, l'équipe ne continuerait plus à maintenir la version 3.5 mais forcerait bientôt un passage obligatoire au moins en version 3.6.x.

Il semble, pour les développeurs, que cette migration forcée en 3.6 constitue un meilleur compromis que de passer directement en version 4. En effet, selon eux, l'interface change très peu entre 3.5 et 3.6, la compatibilité avec d'anciens systèmes ou d'anciennes architectures est garantie contrairement à la version 4 qui ne fonctionne plus, par exemple, avec les systèmes MacOS X 10.4 ou sur les architectures PowerPC. Enfin la plupart des extensions prévues pour la 3.5 resteraient compatibles avec la 3.6.

Il n'en reste pas moins que cette mise à jour « forcée » pourra engendrer des effets de bord indésirables dans certains cas. Le CERTA recommande donc de devancer cette mise à jour obligatoire et de procéder à des tests d'intégration et des vérifications de compatibilité au préalable afin d'éviter tout désagrément lorsque la mise à niveau se produira.

2.1 Documentation :

– Communiqué de Mozilla sur la fin de vie de Firefox 3.5
https://wiki.mozilla.org/Releases/3.5_EOL

3 Gestion des jetons d'authentification dans le protocole ClientLogin de Google

Afin d'accéder à un service Google nécessitant une authentification, une application peut utiliser le protocole `ClientLogin` de Google.

Le principe de ce protocole est de récupérer un jeton d'authentification auprès de Google en lui fournissant un identifiant et un mot de passe. Celui-ci est ensuite envoyé à l'application concernée.

Une vulnérabilité a été identifiée et concerne plusieurs applications installées sur des téléphones fonctionnant sous Android, comme l'application de synchronisation des contacts ou du calendrier. En effet, celles-ci envoient le jeton d'authentification en clair sur le réseau. Il peut alors être récupéré par un attaquant si celui-ci dispose de moyens d'écoute ; ce qui peut être le cas si le téléphone est connecté à un réseau Wi-Fi non sécurisé. Dès lors, en utilisant un mécanisme de rejeu, l'utilisateur malintentionné peut récupérer et modifier les données stockées sur le serveur comme s'il était authentifié.

Le principe de cette attaque n'est pas nouveau et est similaire à la récupération de sessions « HTTP ». Cependant, dans le protocole `ClientLogin`, le jeton engendré est considéré comme valide pendant une durée de deux semaines et n'associe pas un client unique pour chaque jeton.

Google a sorti une mise à jour de son système Android en corrigeant les applications vulnérables avec la version 2.3.4. Comme toutes ces mises à jour, l'utilisateur devra patienter jusqu'à ce que le fabricant et l'opérateur les mettent à disposition. Il semblerait cependant que pour corriger la vulnérabilité, Google forcerait l'utilisation du protocole HTTPS dans les communications entre l'application et le service. L'avantage est que l'utilisateur n'aura pas à attendre une éventuelle mise à jour et que cette solution protègera des attaques contre des applications vulnérables n'ayant pas été identifiées . L'inconvénient est que si l'application ne supporte pas la communication HTTPS, celle-ci ne pourra plus accéder aux services concernés.

Documentation

– Description du mécanisme d'authentification `ClientLogin` :
http://code.google.com/apis/accounts/docs/AuthForInstalledApps.html

4 Le processus `GoogleCrashHandler.exe`

Certains utilisateurs s'étonnent parfois de voir, dans le gestionnaire de processus, une entrée nommée `GoogleCrashHandler.exe`. Ils s'interrogent sur la légitimité du processus, susceptible d'être détecté comme code malveillant par certains antivirus. Il est même possible de voir plusieurs instances de ce programme tourner simultanément, ce qui est parfois caractéristique des codes malveillants.

Il existe bel et bien un programme nommé `GoogleCrashHandler.exe` développé par la société *Google*. Celui-ci a, a priori, deux fonctions principales :

– envoyer de façon « anonyme » des statistiques de l'utilisateur ;
– en cas d'arrêt inopiné d'une application développée par *Google*, envoyer un rapport à l'éditeur, vraisemblablement afin d'identifier un éventuel bogue.

Ce logiciel est installé automatiquement avec toute application *Google* récente. Chacune d'entre elles peut déclencher le lancement d'une instance de `GoogleCrashHandler.exe`. L'exécution de ce programme est liée à l'activation d'une option d'envoi automatique des statistiques d'usage et de rapport de crash. Par exemple, sous *Google Chrome*, cette option peut être désactivée via le panneau des options avancées (cela se fait en décochant une case). Pour rester dans l'exemple de *Google Chrome*, au moment de l'installation du navigateur, l'activation automatique est proposée par défaut.

Pour empêcher le lancement du processus `GoogleCrashHandler.exe`, il faut donc penser à le désactiver pour chaque application *Google* qui l'utilise. Le principal risque associé à ce programme est la fuite d'informations, notamment en cas d'arrêt inopiné d'un logiciel.

5 Liens utiles

– Mémento sur les virus :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
– Note d'information du CERTA sur l'acquisition de correctifs :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
– Note d'information du CERTA sur les systèmes obsolètes :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
– Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
– Note d'information du CERTA sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
– Note d'information sur la terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
– Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
http://www.auscert.org.au/render.html?it=1937
– Note d'information du CERTA sur les risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
– Note d'information du CERTA sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

6 Rappel des avis émis

Dans la période du 13 au 19 mai 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-289 : Vulnérabilité dans HP Network Node Manager i
- CERTA-2011-AVI-290 : Vulnérabilités dans Adobe Flash Player
- CERTA-2011-AVI-291 : Vulnérabilité dans CA eHealth
- CERTA-2011-AVI-292 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-293 : Vulnérabilité dans IBM Datacap Taskmaster Capture
- CERTA-2011-AVI-294 : Vulnérabilités dans Adobe Flash Media Server
- CERTA-2011-AVI-295 : Vulnérabilités dans Citrix XenServer
- CERTA-2011-AVI-296 : Vulnérabilité dans Apache Portable Runtime
- CERTA-2011-AVI-299 : Vulnérabilité dans IBM Informix
- CERTA-2011-AVI-300 : Vulnérabilité dans HP Business Availibility Center
- CERTA-2011-AVI-301 : Vulnérabilité dans Apache Tomcat
- CERTA-2011-AVI-302 : Vulnérabilité dans Opera

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

- CERTA-2011-AVI-079-007 : Vulnérabilité dans plusieurs implémentations de Java (ajout de la référence au bulletin Hitachi HS11-008)
- CERTA-2011-AVI-273-001 : Vulnérabilité dans Vino (ajout des correctifs Fedora)
- CERTA-2011-AVI-277-001 : Multiples vulnérabilités dans HP SNMP Agents et HP Insight Management Agents (modification des produits affectés suite à la mise à jour du bulletin HP c02735590)
- CERTA-2011-AVI-280-001 : Vulnérabilité dans Exim (ajouts des correctifs Fedora)
- CERTA-2011-AVI-283-001 : Vulnérabilité dans Postfix (ajout des correctifs Fedora)
- CERTA-2011-AVI-297-001 : Vulnérabilité dans Debian Exim (ajout des correctifs Fedora)
- CERTA-2011-AVI-298-001 : Vulnérabilités dans GuppY (modification des sections Risque, Résumé et Description)

7 Actions suggérées

7.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

7.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

7.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

7.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

7.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

7.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

7.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

8 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

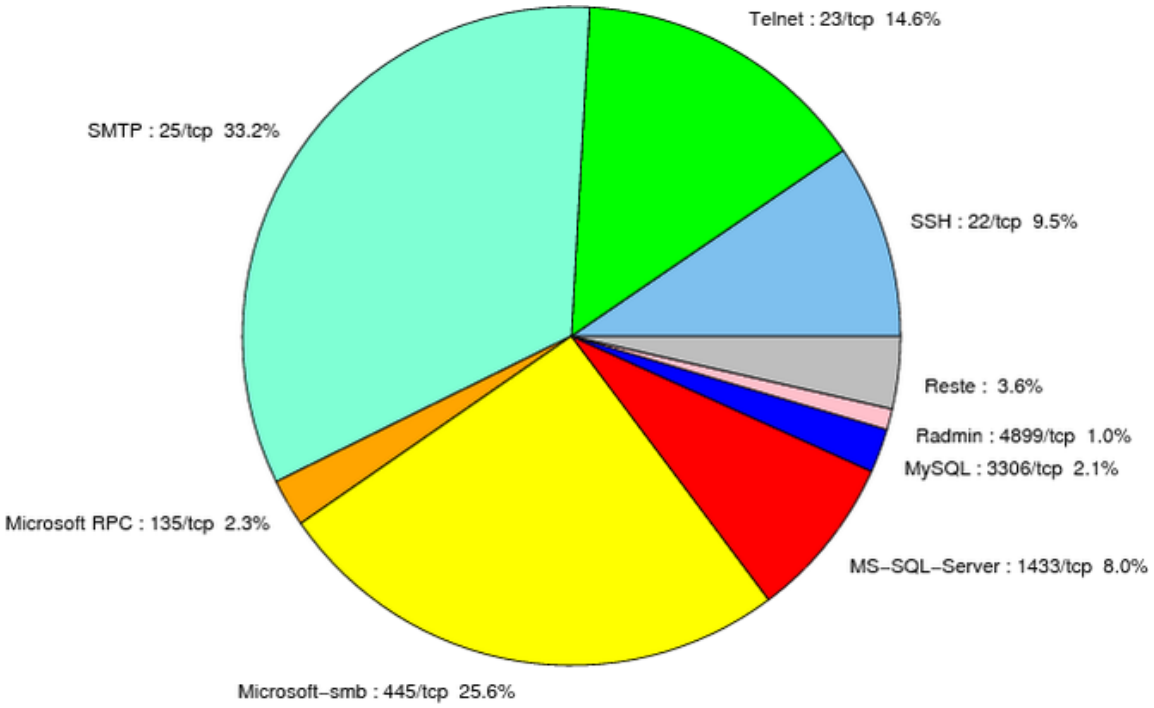

FIG. 1: Répartition relative des ports pour la semaine du 13 au 19 mai 2011

port	pourcentage
25/tcp	33.17
445/tcp	25.6
23/tcp	14.67
22/tcp	9.53
1433/tcp	8.03
80/tcp	5.23
135/tcp	2.33
3306/tcp	2.14
4899/tcp	1.02
3389/tcp	0.93
3128/tcp	0.65
21/tcp	0.56
1434/udp	0.37
1080/tcp	0.09

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

20 mai 2011 version initiale.