



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 30 septembre 2011  
N° CERTA-2011-ACT-039

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2011-39**

---

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-2011-ACT-039>

---

### Gestion du document

Référence	CERTA-2011-ACT-039
Titre	Bulletin d'actualité 2011-39
Date de la première version	30 septembre 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-039.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-039/>

## 1 Attaques récentes sur SSLv3.0/TLSv1.0

### 1.1 Contexte

Récemment, deux chercheurs ont dévoilé une nouvelle attaque visant les protocoles SSLv3.0 et TLSv1.0. Cette attaque, dénommée *BEAST* par ses auteurs, permet à un attaquant de décrypter à la volée, sous certaines conditions, une partie du trafic chiffré.

Elle repose sur une faiblesse des algorithmes de chiffrement par blocs chaînés (*Cypher Block Chaining* ou CBC) connue depuis de nombreuses années. Cette vulnérabilité est en partie à l'origine de la création de TLSv1.1. Afin de bien comprendre le fonctionnement de cette faiblesse, il convient de rappeler le principe des algorithmes de chiffrement de type CBC.

### 1.2 Le chiffrement CBC

Lors de l'utilisation d'un algorithme de chiffrement de type CBC, les données à traiter sont, dans un premier temps, découpées en blocs de tailles identiques (dépendantes de l'algorithme et des longueurs de clés utilisées).

Le chiffrement s'effectue ensuite sur chacun de ces blocs. Cependant, afin d'éviter que deux blocs identiques aient un chiffré identique, chacun des blocs est préalablement transformé. Cette transformation est usuellement une opération « ou exclusif » et fait intervenir un bloc spécial, appelé vecteur d'initialisation, propre à chaque bloc de données à chiffrer. L'algorithme de chiffrement est donc une fonction de la clé, du texte clair et du vecteur d'initialisation.

La création de ces vecteurs d'initialisation peut être effectuée de différentes façons. Dans le cadre de SSLv3.0 et TLSv1.0, le bloc d'initialisation est simplement le résultat du chiffrement du bloc précédent. Le premier bloc d'initialisation est, quant à lui, aléatoire.

### 1.3 Principe de l'attaque

Nous nous plaçons ici dans le cas où le vecteur d'initialisation utilisé à l'étape N est le résultat du chiffrement à l'étape N-1.

La connaissance de l'ensemble du chiffré permet de déterminer à chaque étape, sauf la première, le vecteur d'initialisation utilisé. Il devient alors possible de vérifier diverses hypothèses quant au contenu du texte clair et de mener des attaques par force brute.

Bien entendu, ce type d'attaque n'est pas envisageable dans la pratique. Cependant, il est possible d'exploiter le principe de base afin d'obtenir des résultats dans un temps raisonnable.

Supposons connaître pour un bloc donné sa version chiffrée, le vecteur d'initialisation associé ainsi que l'ensemble des octets du bloc non chiffré moins un octet. Il devient alors évident qu'une attaque par force brute pour déterminer l'octet manquant est tout à fait possible (il suffit de tester 256 possibilités différentes).

Ce type d'attaque est intéressant dans le cas où un attaquant est capable de demander le chiffrement de données connues auxquelles sera concaténé un secret (non connu de l'attaquant) : en modifiant la taille des données qu'il fournit, l'attaquant est capable de se ramener au cas précédemment exposé. Il pourra alors décrypter le secret.

### 1.4 Application pratique

L'attaque décrite ci-dessus s'adapte très bien au protocole HTTPS et au vol de fichiers de session (cookies). En effet, lors de l'envoi d'une requête HTTPS vers un serveur, le navigateur concatène automatiquement à la requête l'ensemble des cookies dont il dispose pour le domaine cible. Ainsi, en faisant varier la longueur de l'adresse réticulaire demandée, l'attaquant est capable d'obtenir un bloc contenant une partie de la requête effectuée (connue) et le premier caractère du cookie (non-connu). Une fois ce caractère déterminé, il modifie de nouveau la taille de l'URL cible pour obtenir un nouveau bloc contenant le second caractère du cookie et ainsi de suite jusqu'à obtenir l'ensemble du cookie. Bien entendu, cette technique nécessite que l'utilisateur victime soit connecté au serveur cible et que l'attaquant dispose d'un moyen d'effectuer des requêtes vers ce serveur depuis la machine de la victime. Il lui est aussi nécessaire d'intercepter le trafic chiffré.

### 1.5 Mesures de protection

La faiblesse exploitée ici réside dans le type de chiffrement utilisé dans le cadre des transactions chiffrées : le chiffrement par blocs chaînés. Il est donc recommandé de ne pas utiliser ce type de chiffrement et de lui préférer un chiffrement par flux. D'autres parts, une migration vers une version supérieure à 1.0 du protocole TLS règle ce problème.

Des correctifs sont aussi disponibles (ou en cours de développement) pour les différents produits concernés. Il est conseillé d'appliquer ces mises à jour au plus vite.

Le CERTA rappelle qu'il est impératif de ne pas effectuer d'opérations sensibles sur l'Internet depuis un réseau non sûr.

## Documentation

- Avis de sécurité Microsoft 2588513 du 26 septembre 2011 :  
<http://technet.microsoft.com/en-us/security/advisory/2588513>
- Rapport de bug Mozilla 665814 du 20 juin 2011 :  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=665814](https://bugzilla.mozilla.org/show_bug.cgi?id=665814)
- CVE référence CVE-2011-3389 :  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389>

## 2 Élévation de privilèges d'administrateur local à administrateur de domaine (2ème partie)

Lors du premier volet de cette série d'articles, nous avons abordé l'élévation de privilège d'administration locale vers l'administration Active Directory. Un profil spécifique d'attaquant va déployer de grands efforts afin de parvenir à ce niveau de privilège : le voleur d'informations.

Ainsi, depuis le poste d'un simple utilisateur compromis via une simple pièce jointe type PDF ou un site malveillant, l'attaquant obtient (trop souvent facilement) le contrôle d'un ou plusieurs compte d'administration du domaine. A ce stade, l'attaquant détient les clés lui permettant d'accéder aux données de tous les utilisateurs du domaine : le comité exécutif, le cabinet d'un ministère, un chercheur. . .

En effet, les informations que l'attaquant recherche peuvent être disséminées dans différents systèmes : les serveurs de fichiers ou de messagerie, les dossiers personnels sur un portable, les différentes applications métier. L'obtention des privilèges d'administration du domaine va permettre à l'attaquant d'accéder sans effort à toutes les données du système d'information dont le contrôle d'accès est assuré via Active Directory.

Reprenons notre énumération des attaques rencontrées.

### Simple et Rapide: Récupération des secrets LSA

#### Attaque :

Depuis des années, des outils existent pour extraire les secrets d'une machine. Parmi ces secrets, on va retrouver par exemple :

- les mots de passe des comptes configurés sur le poste :
  - pour démarrer un service ;
  - pour exécuter une tâche planifiée ;
  - associés aux applications COM+.
- les clés de chiffrement associées au profil de la machine.

Ces outils donnent immédiatement accès à tous les mots de passe (chiffrés de façon réversible). Ils peuvent être immédiatement utilisés.

Il est important de bien comprendre que cette extraction de secrets n'est accessible qu'aux seuls administrateurs d'un poste. Ces outils n'exploitent donc pas de vulnérabilités du système d'exploitation. Par définition, l'administrateur d'un système a accès à tous les secrets de celui-ci.

#### Prévention :

Cette attaque met en évidence un principe simple : lorsque l'on confie un secret à une machine, on le confie implicitement à tous les administrateurs de cette machine. Si un secret d'une machine (compte de service sur un portable, tâche planifiée sur un serveur) expose un secret aussi puissant qu'un mot de passe d'administration du domaine, il conviendra d'en restreindre strictement l'accès physique ainsi que les droits d'administration.

### Simple et Rapide : Pass the hash

#### Attaque :

Le processus LSASS détient les condensats des mots de passe de différentes sessions ouvertes sur le système. Les outils de type « Pass the hash » permettent à l'attaquant de rejouer des authentications en utilisant ce condensat. Cette attaque est assez proche de l'attaque « énumération des sessions de la machine compromise » décrite la semaine dernière avec l'avantage important de ne pas être liée à une machine. Le condensat du mot de passe peut être réutilisé sur n'importe quel système du domaine tant que le mot de passe n'est pas changé.

#### Prévention :

La prévention de cette attaque est identique à l'attaque « énumération des sessions » :

- ne pas ouvrir de session interactive avec un compte d'administration « puissant » sur des postes d'utilisateurs. Au contraire, utiliser RunAs ou « exécuter en tant que » pour élever les privilèges des seuls processus nécessaires ;
- ne pas utiliser de compte d'administration du domaine pour intervenir sur des postes utilisateur potentiellement compromis (recommandation typiquement destinée aux équipes de support).

Plus spécifiquement sur cette attaque, on s'attachera à renouveler régulièrement les mots de passe des comptes puissants.

### **3 Rappel des avis émis**

Dans la période du 23 au 29 septembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-532 : HP Business Service Automation Essentials
- CERTA-2011-AVI-533 : Multiples vulnérabilités dans SPIP
- CERTA-2011-AVI-534 : Vulnérabilités dans FFmpeg
- CERTA-2011-AVI-535 : Vulnérabilité dans Opera

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

- CERTA-2011-AVI-506-001 : Vulnérabilités dans MantisBT (ajout de références CVE)

### **4 Actions suggérées**

#### **4.1 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 réglementaire, 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.

#### **4.2 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.

#### **4.3 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.

#### **4.4 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.

## 4.5 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.

## 4.6 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 inexplicables 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.

## 4.7 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](http://www.ssi.gouv.fr/site_rubrique62.html)

## 5 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.

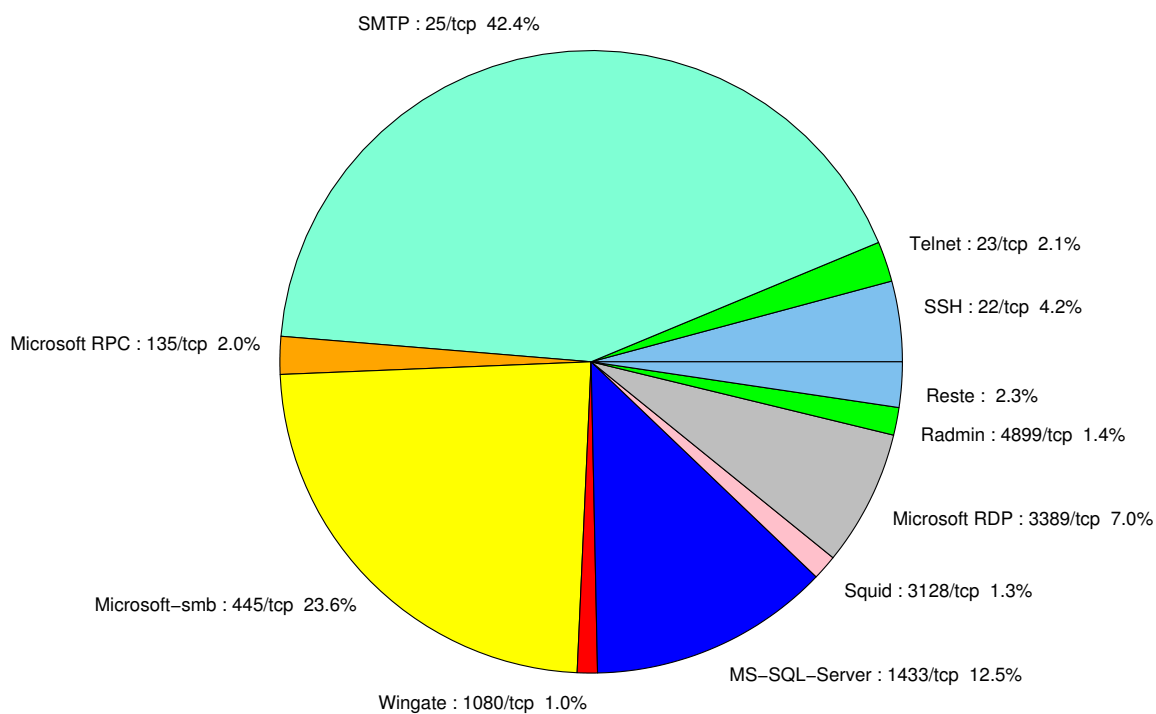


FIG. 1: Répartition relative des ports pour la semaine du 23 au 29 septembre 2011

port	pourcentage
25/tcp	42.42
445/tcp	23.62
1433/tcp	12.53
80/tcp	7.57
3389/tcp	7.04
22/tcp	4.17
23/tcp	2.08
135/tcp	1.95
4899/tcp	1.43
3128/tcp	1.3
1080/tcp	1.04
2967/tcp	0.65
3306/tcp	0.52

TAB. 2: Paquets rejetés

## Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

## Gestion détaillée du document

30 septembre 2011 version initiale.