Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2012
N° CERTA-2012-ACT-038

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-038

Gestion du document

Référence	CERTA-2012-ACT-038
Titre	Bulletin d'actualité CERTA-2012-ACT-038
Date de la première version	21 septembre 2012
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.

1 Vulnérabilité critique dans Internet Explorer

Cette semaine, le CERTA a diffusé l'alerte CERTA-2012-ALE-006 concernant une vulnérabilité majeure dans Microsoft Internet Explorer. Des codes d'exploitation ont rapidement circulé sur l'Internet, et sont actuellement utilisés par un nombre grandissant d'attaquants par l'intermédiaire de sites Web compromis ou malveillants.

Cette vulnérabilité permet d'exécuter du code arbitraire à distance. Il s'agit d'un *Use-After-Free* dans *mshtml.dll*. Cette bibliothèque, aussi connue sous le nom de Trident, est le moteur de rendu de Microsoft Internet Explorer ; il effectue le traitement du CSS, du HTML, et du Javascript des pages Web.

Microsoft a depuis publié des correctifs provisoires ; au moment de la rédaction de ce bulletin (vendredi 21 septembre 2012 17h00 GMT+1), l'éditeur a annoncé la publication imminente d'un correctif définitif. Le CERTA recommande son application au plus tôt. Dans l'intervalle, se reporter à l'alerte en référence pour les mesures de contournement provisoire.

Pour aller plus loin dans la reflexion SSI sur la prise en compte des menaces liées aux vulnérabilités 0day sur les navigateurs, se reporter à l'article suivant de ce bulletin d'actualité.

Documentation

– CERTA-2012-ALE-006-002 : Vulnérabilité dans Internet Explorer :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-006/index.html

2 Navigateurs Internet : prévention des attaques 0day

Force est de constater que les attaques contre les navigateurs ne ralentissent pas. La dernière alerte de sécurité, émise par Microsoft, sur une faille 0day Internet Explorer exploitée permet d'aborder à nouveau ce sujet.

Par définition, une vulnérabilité 0day peut être exploitée par des attaquants avant que l'éditeur, qui en ignore parfois l'existence, ait eu le temps de la corriger. Ces vulnérabilités posent un vrai défi aux personnes chargées de SSI. Cet article ne peut donc apporter de solution simple et unique à ce problème, mais propose une approche éprouvée dans le cadre des incidents traités par le CERTA.

Les vulnérabilités 0day sont dévoilées sans préavis, et les solutions provisoires de contournement proposées par les éditeurs et les CERTs sont souvent complexes et sont susceptibles d'avoir des effets de bord significatifs sur le système d'information. Ces solutions transitoires sont parfois difficiles à mettre en place dans l'urgence, comme notamment le déploiement d'un navigateur alternatif à celui ciblé par le 0day :

- déploiement d'un nouveau logiciel sans les « garde-fous » usuels d'un projet (tests, intégration, étude d'impact, périmètre, etc.) ;
- information des utilisateurs sur la nécessité d'utiliser différents navigateurs, notamment sur les applications métier requérant un navigateur spécifique ;
- mise en place des mesures de contrôle, afin de s'assurer de l'usage du navigateur non vulnérable lors de la navigation sur Internet (par exemple le blocage au périmètre des *User Agents* vulnérables).

Cette démarche d'anticipation des attaques 0day est également préférable pour la mise en place de solutions de durcissement du navigateur (tel EMET), d'invalidation de greffons (dans le cas de vulnérabilité java par exemple), ou de filtrage de ports réseau (pour des vulnérabilités critiques de systèmes d'exploitation). Elle nécessite de concevoir, tester et déployer de manière proactive des solutions génériques de secours.

Quelques pistes peuvent être envisagées pour se préparer aux futurs 0day :

- déployer et maintenir à jour plusieurs navigateurs sur chaque poste. Pour accompagner cette mesure, il faut pouvoir informer rapidement les utilisateurs de changer de navigateur principal, filtrer les *user-agent* au niveau du proxy, vérifier le comportement des sites intranet avec ces navigateurs et les modifier le cas échéant. Il est également possible d'avoir sur les postes un navigateur dédié à l'usage de l'intranet, et d'autres réservés pour la navigation sur l'Internet. Cette solution peut résoudre certaines situations où l'intranet nécessite un greffon obsolète (java...) ;
- mesurer l'impact sur les applications métier de la desactivation de greffons, de scripting (javascript...), et de *handlers* (appel du navigateur à des logiciels tiers), afin de pouvoir décider en connaissance de cause lors d'une alerte ;
- limiter les droits des utilisateurs : supprimer les droits d'administration, appliquer les *Software Restriction Policies*. Ces bonnes pratiques limitent la capacité de nuisance de l'attaquant qui pénétrerait via un 0day ;
- installer et configurer EMET sur tous les postes utilisateur ;
- renforcer la sécurité périmètrique: configuration restrictive du pare-feu, lecture et exploitation des journaux proxy et pare-feu ;
- sensibiliser les utilisateurs aux principaux vecteurs d'attaque, comme les liens html dans les courriels, ou la navigation sur des sites Web suspects.

L'anticipation de ce type d'incident dans une logique de défense en profondeur est donc la clé de voûte d'une réponse efficace contre ces menaces.

3 Une mise à jour des antivirus Sophos sème le désordre

L'éditeur *Sophos* a publié, le 19 septembre 2012, une mise à jour de sa base de signatures qui a provoqué une vague de faux positifs de détection de codes malveillants. Plus précisément, ce sont les logiciels possédant une fonctionnalité de mise-à-jour automatique qui apparaissent comme étant infectés par le virus *Shh/Updater-B*. Les antivirus *Sophos* se détectent eux-mêmes comme étant malveillants.

Les conséquences de cette situation sont critiques : les applications ne peuvent plus se mettre à jour et certaines d'entre elles cessent tout bonnement de fonctionner, ce qui se traduit par un déni de service ; de plus, l'antivirus lui-même ne peut plus se mettre à jour, empêchant le déploiement de la nouvelle base de signatures corrigée par Sophos. Ce problème devient encore plus épineux lorsque l'antivirus est configuré pour effacer automatiquement les fichiers en cas d'alerte d'infection.

La reprise sur ce type d'incident est particulièrement complexe. *Sophos* propose, dans un article publié sur son site, plusieurs solutions pour rendre utilisable la fonctionnalité de mise-à-jour de l'antivirus et télécharger les dernières signatures qui neutralisent les détections intempestives de *Shh/Updater-B*. Cependant, ces solutions

ne fonctionnent que si les fichiers anormalement détectés comme malveillants ont été placés en quarantaine. Ils ne peuvent sortir de quarantaine qu'une fois l'antivirus mis à jour. Par contre, si la configuration de l'antivirus provoque la suppression automatique des fichiers considérés comme malveillants, il devient nécessaire de réinstaller les applications importées.

Le CERTA recommande donc, d'une manière générale, de configurer les antivirus pour mettre en quarantaine les fichiers considérés comme malveillants plutôt que de les supprimer.

Documentation

- Article de Sophos concernant les faux-positifs *Shh/Updater-B* :
  http://nakedsecurity.sophos.com/2012/09/19/sshupdater-b-fsophos-anti-virus-products/
- Procédure Sophos de correction du problème :
  http://www.sophos.com/en-us/support/knowledgebase/118311.aspx
  http://www.sophos.com/fr-fr/support/knowledgebase/118311.aspx

4 Rappel des avis émis

Dans la période du 14 au 20 septembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-502 : Vulnérabilité dans Cisco ASA-CX et PRSM
- CERTA-2012-AVI-503 : Vulnérabilité dans Cisco Unified Presence et Jabber Extensible Communication Platform
- CERTA-2012-AVI-504 : Vulnérabilité dans Citrix Receiver
- CERTA-2012-AVI-505 : Multiples vulnérabilités dans Google Chrome pour Android
- CERTA-2012-AVI-506 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2012-AVI-507 : Multiples vulnérabilités dans système SCADA Siemens WinCC
- CERTA-2012-AVI-508 : Vulnérabilité dans le système SCADA Siemens S7-1200
- CERTA-2012-AVI-509 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-511 : Multiples vulnérabilités dans Moodle

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

- CERTA-2012-ALE-006-002 : Vulnérabilité dans Internet Explorer (ajout d'un contournement provisoire, ajout et modification des documentations)
- CERTA-2012-AVI-510-001 : Vulnerabilité dans eZ-Publish (correction URL)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

5.4 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.

5.5 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.

5.6 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.

5.7 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

Gestion détaillée du document

21 septembre 2012 version initiale.