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 juin 2012
N° CERTA-2012-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-25

Gestion du document

Référence	CERTA-2012-ACT-025
Titre	Bulletin d'actualité 2012-25
Date de la première version	21 juin 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 Publication du guide de sécurisation des systèmes industriels

Un guide sur la cybersécurité des systèmes industriels a été publié par l'ANSSI le 19 juin 2012. Ce guide est le produit d'une large concertation en 2011, entre les ministères et les industriels concernés. Il présente une méthodologie de sécurisation de ces systèmes illustrée de cas concrets.

Cette concertation fait suite à une prise de conscience des différents acteurs du domaine de la vulnérabilité des systèmes industriels face aux cyber attaques (vol de donnée, indisponibilité, etc.). L'exemple du ver Stuxnet en 2010 a montré que le niveau de sécurité de ces systèmes est souvent très insuffisant, et que la criticité de certains d'entre eux en font des cibles de choix d'attaques informatiques.

Le CERTA recommande aux RSSI concernés la lecture et l'application des mesures préconisées dans ce guide, l'implication de la SSI dans les projets visant des systèmes industriels et la prise en compte des risques associés dans la PSSI de l'entreprise.

– La cybersécurité des systèmes industriels :
  http://www.ssi.gouv.fr/systemesindustriels

2 EMET v3

EMET (Enhanced Mitigation Experience Toolkit), présenté dans le bulletin d'actualité CERTA-2012-ACT-016, a fait l'objet d'une mise à jour avec la publication de la version 3. Pour rappel, EMET est un outil développé par

Microsoft permettant, dans certains cas, de rendre plus difficile l'exploitation d'une vulnérabilité dans un logiciel fonctionnant sous Windows.

La principale fonctionnalité apportée par cette mise à jour est la possibilité de déploiement et de configuration *via* les GPO (stratégies de groupe), ce qui facilite grandement son utilisation en environnement Active Directory. En particulier, des profils par défaut permettent d'activer les protections pour l'ensemble des produits Microsoft.

Enfin, l'introduction d'une fonctionnalité de journalisation et de notification permet une détection plus facile d'éventuelles tentatives d'exploitation de vulnérabilités.

Documentation

- Bulletin d'actualité CERTA-2012-ACT-016 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-016/index.html
- Introducing EMET v3 :
  http://blogs.technet.com/b/srd/archive/2012/05/15/introducing-emet-v3.aspx
- Trousse à outils EMET :
  http://support.microsoft.com/kb/2458544/fr
- Téléchargement d'EMET v3 :
  http://go.microsoft.com/fwlink/?LinkID=200220&clcid=0x409

3 Risque accru d'exploitation de vulnérabilités dans Internet Explorer

La vulnérabilité présentée dans CERTA-2012-ALE-003, toujours non corrigée à la parution de ce bulletin, a fait l'objet d'une publication d'un code d'exploitation dans le logiciel Metasploit, visant Internet Explorer. Metasploit est l'un des outils d'attaque public les plus connus. Ses codes d'attaque sont souvent réutilisés, ce qui augmente nettement le risque de compromission.

De plus, de nombreux acteurs, notamment Microsoft et Google, ont annoncé avoir constaté une exploitation active de la vulnérabilité.

Le CERTA recommande donc de mettre en œuvre au plus tôt l'une des méthodes de contournement suivantes afin de se protéger :

- appliquer le contournement bloquant le vecteur d'attaque (*Fix it*) ;
- déployer Enhanced Mitigation Experience Toolkit (EMET) ;
- configurer Internet Explorer de manière à obtenir un avertissement avant d'exécuter Active Scripting ou désactiver Active Scripting dans les zones de sécurité à risque (Internet et potentiellement Intranet Local);
- utiliser un autre navigateur.

De même, Metasploit inclut un code permettant d'exploiter l'une des treize vulnérabilités corrigées la semaine dernière dans Internet Explorer (avis CERTA-2012-AVI-321). Celle-ci est également exploitée activement et il n'est pas à exclure que d'autres le soient également dans les prochains jours. Il est donc nécessaire d'appliquer les correctifs sans délai.

Documentation

- Alerte du CERTA CERTA-2012-ALE-003 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-003/index.html
- *Fix It* Vulnérabilité Microsoft XML Core Services :
  http://support.microsoft.com/kb/2719615
- Divers liens relatant l'exploitation active des vulnérabilités :
  http://nakedsecurity.sophos.com/2012/06/19/ie-remote-code-execution-vulnerability-being-actively-exploited-in-the-wild/
  http://nakedsecurity.sophos.com/2012/06/20/aeronautical-state-sponsored-exploit/
  http://googleonlinesecurity.blogspot.co.uk/2012/06/microsoft-xml-vulnerability-under.html
- Avis du CERTA CERTA-2012-AVI-321 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-321/index.html

4 Rappel des avis émis

Dans la période du 15 au 21 juin 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-334 : Vulnérabilité dans FreeBSD
- CERTA-2012-AVI-335 : Vulnérabilité dans HP OpenVMS
- CERTA-2012-AVI-336 : Vulnérabilités dans SPIP
- CERTA-2012-AVI-337 : Vulnérabilité dans Asterisk
- CERTA-2012-AVI-338 : Multiples vulnérabilités dans Opera
- CERTA-2012-AVI-339 : Vulnérabilité dans Symantec LiveUpdate Administrator
- CERTA-2012-AVI-340 : Vulnérabilité dans des produits Mozilla
- CERTA-2012-AVI-341 : Multiples vulnérabilités dans PHP
- CERTA-2012-AVI-342 : Vulnérabilité dans IBM Lotus Notes
- CERTA-2012-AVI-343 : Vulnérabilités dans Libtiff
- CERTA-2012-AVI-344 : Vulnérabilités dans Joomla!
- CERTA-2012-AVI-345 : Multiples vulnérabilités dans Cisco AnyConnect Secure Mobility Client
- CERTA-2012-AVI-346 : Vulnérabilité dans Cisco Application Control Engine
- CERTA-2012-AVI-347 : Vulnérabilité dans Cisco ASA 5500 et Cisco Catalyst 6500

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

Une faille connue publiquement et non-corrigée est une porte d'entrée sur un système d'information. Ce sont les cibles privilégiées des attaquants. Ils possèdent en effet tous les détails techniques nécessaires pour réaliser une exploitation de ces vulnérabilités. De nombreux malwares scannent également activement l'Internet à la recherche de ces failles. Il convient donc de corriger le plus rapidement possible les vulnérabilités signalées par les éditeurs.

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

Les codes malveillants peuvent également chercher à ouvrir des ports spécifiques ou à utiliser ceux ouverts par une compromission antérieure 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 suspecte sur votre système d'information.

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/fr/anssi/formation/

Gestion détaillée du document

21 juin 2012 version initiale.