Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juin 2012
N° CERTA-2012-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-26

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-026

Gestion du document

Référence	CERTA-2012-ACT-026
Titre	Bulletin d'actualité 2012-26
Date de la première version	29 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 Vulnérabilité de l'instruction SYSRET sur les processeurs INTEL

Les instructions SYSCALL et SYSRET sont utilisées par la plupart des systèmes d'exploitation 64 bits pour déclencher un appel système et en revenir. L'instruction SYSRET est décrite Chapitre 4, page 599 du manuel de développement Intel (voir section Documentation).

Une vulnérabilité de l'instruction SYSRET sur les processeurs Intel a été récemment découverte par Rafal Wojtczuk. L'exploitation de cette faille peut conduire, sur certains systèmes d'exploitation, à une élévation de privilèges. Ce bogue n'affecte que les processeurs Intel et pas les processeurs AMD.

Description technique

Contrairement au mécanisme classique de déclenchement d'appel système reposant sur une interruption logicielle, l'instruction SYSRET ne restaure pas le pointeur de pile utilisateur. Le noyau doit donc réaliser cette opération avant d'appeler l'instruction SYSRET.

Le problème réside dans l'implémentation par Intel du standard x86-64, dans laquelle l'instruction SYSRET peut déclencher une exception au niveau du processeur sous certaines conditions. Le processeur utilise alors la pile utilisateur préalablement restaurée pour empiler automatiquement des registres liés à l'exception. Cette vulnérabilité permet à un attaquant de modifier des structures du noyau depuis l'espace utilisateur afin de réaliser une élévation de privilèges.

L'attaque consiste à réunir les conditions nécessaires au déclenchement de l'exception puis à modifier le pointeur de pile utilisateur de sorte qu'il pointe vers les structures du noyau visées.

Cette vulnérabilité avait déjà été découverte et corrigée en 2006 (CVE-2006-0744) sur les noyaux Linux, mais l'intitulé de l'alerte d'alors suggérait que seul Linux était affecté.

Pour les autres systèmes, le CERTA recommande d'appliquer dès que possible les correctifs.

Systèmes concernés et systèmes immunes

Les systèmes suivants sont affectés par cette vulnérabilité :

- Xen, toutes les versions 64 bits sur processeur Intel avant les correctifs du 12 juin 2012 ;
- FreeBSD, toutes les versions 64 bits sur processeur Intel avant les correctifs du 12 juin 2012 ;
- NetBSD, toutes les versions 64 bits sur processeur Intel avant les correctifs du 12 juin 2012 ;
- OpenBSD jusqu'à la version 4.9, en 64 bits sur processeur Intel ;
- Microsoft, versions 64 bits de Windows 7 et de Windows Server 2008 R2 (CVE-2012-0217) avant les correctifs du 12 juin 2012.

Les systèmes suivants ne sont pas affectés :

- OpenBSD 5.0 et versions suivantes ;
- l'ensemble des systèmes tournant sur processeur AMD ;
- les noyaux Linux postérieurs à la version 2.6.16.5 du fait des correctifs CVE-2005-1764 et CVE-2006-0744.

Documentation

- *Intel 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference, M-Z* : http://download.intel.com/products/processor/manual/253667.pdf
- Détails techniques et résolution : http://blog.xen.org/index.php/2012/06/13/the-intel-sysret-privilege-escalation/
- Avis du CERTA CERTA-2012-AVI-326 du 13 juin 2012 : http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-326/index.html
- Avis du CERTA CERTA-2012-AVI-328 du 13 juin 2012 : http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-328/index.html
- Avis du CERTA CERTA-2012-AVI-334 du 15 juin 2012 : http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-334/index.html
- Bulletin de sécurité RedHat RHSA-2012:0720 du 12 juin 2012 : http://rhn.redhat.com/errata/RHSA-2012-0720.html
- Bulletin de sécurité RedHat RHSA-2012:721 du 12 juin 2012 : http://rhn.redhat.com/errata/RHSA-2012-721.html
- Note de vulnérabilité de l'US-CERT VU#649219 du 25 juin 2012 : http://www.kb.cert.org/vuls/id/649219
- Référence CVE CVE-2005-1764 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1764
- Référence CVE CVE-2006-0744 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0744
- Référence CVE CVE-2012-0217 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0217

2 Vulnérabilité critique de l'extension JCE de Joomla

JCE (*Joomla! Content Editor*) est une extension du *Joomla! Content Management System*. Cette extension est sujette à plusieurs vulnérabilités rendant le dêpot d'un *phpshell* possible par un attaquant. La vulnérabilité a été déclarée à Joomla le 21 janvier 2011 et les versions supérieures à 1.5.7.7 et 1.1.9.3 incluses ont été corrigées. Beaucoup d'extensions JCE de version inférieure à 1.5.7.7 et 1.1.9.3 sont encore utilisées et plusieurs sites Web ont été récemment défigurés en exploitant ces vulnérabilités. Un outil d'exploitation automatique est disponible sur l'Internet. Ce dernier vérifie que la version de l'extension JCE est inférieure à 1.5.7.10 avant de tenter d'exploiter les vulnérabilités potentiellement présentes. Il est possible de repérer une exploitation réussie de ces vulnérabilités

en examinant les journaux. Le scan de la version de JCE peut être repéré par l'url suivante dans les journaux d'accès du serveur Web :

```
GET //index.php?option=com_jce&task=plugin&plugin=imgmanager
&file=imgmanager&version=1576&cid=20
```

Le dépôt de la charge peut se voir aussi dans les journaux d'accès du serveur Web :

```
 POST //index.php?option=com_jce&task=plugin&plugin=imgmanager
&file=imgmanager&method=form
&cid=20&6bc427c8a7981f4fe1f5ac65c1246b5f=9d09f693c63c1988a9f8a564e0da7743
```

La charge déposéee se nomme « 0day.php » mais ce nom est susceptible de changer.

Le CERTA recommande de rechercher les traces dans les journaux d'une possible exploitation de ces vulnérabilités. En cas de compromission, il est nécessaire de réinstaller la machine. La mise à jour de l'extension JCE est aussi recommandée pour se prémunir de cette attaque.

3 Rançongiciel aux couleurs de l'ANSSI

Depuis plusieurs mois, de nombreux internautes sont victimes d'un code malveillant bloquant leur ordinateur. Ce code affiche une page qui comporte le logo de la gendarmerie, parfois celui de la police (OCLCTIC) et plus récemment celui de l'ANSSI. Le code malveillant tente d'empêcher toute action sur l'ordinateur infecté et exige le paiement d'une pseudo-amende de 100 Euros.

Aucune entité gouvernementale ne chiffrerait le disque dur d'un internaute ni ne le forcerait à payer une amende par l'intermédiaire d'un site non gouvernemental. Il ne faut donc en aucun cas payer la rançon. Dans le cadre d'une infection d'un poste de travail professionnel, des documents importants stockés sur le poste pourraient être perdus.

La mise à jour du navigateur ainsi que des plug-ins de contenu tels que Flash ou Java protégera de ce type d'attaque, diffusée principalement par l'intermédiaire de bannières publicitaires. En cas d'infection, la restauration d'un point de sauvegarde Windows peut éventuellement corriger les fichiers systèmes altérés par le code malveillant et en annuler les effets. Enfin, la sauvegarde régulière des documents importants sur un serveur préviendra une perte de données due à ce type de code malveillant.

Articles sur les autres sites de l'ANSSI :

- http://www.ssi.gouv.fr/fr/menu/actualites/attention-arnaque-en-ligne.html
- http://www.securite-informatique.gouv.fr/gp_article781.html

4 Rappel des avis émis

Dans la période du 22 au 28 juin 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-348 : Vulnérabilité dans F5 BIG-IP
- CERTA-2012-AVI-349 : Vulnérabilités dans IBM System Storage DS Storage Manager
- CERTA-2012-AVI-350 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-351 : Multiples vulnérabilités dans IBM Lotus Expeditor
- CERTA-2012-AVI-352 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-353 : Vulnérabilité dans AIX
- CERTA-2012-AVI-354 : Vulnérabilité dans IMP
- CERTA-2012-AVI-355 : Multiples vulnérabilités dans Symantec Message Filter
- CERTA-2012-AVI-356 : Multiples vulnérabilités dans Cisco WebEx Player

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

29 juin 2012 version initiale.