Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juin 2012
N° CERTA-2012-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-24

Gestion du document

Référence	CERTA-2012-ACT-024
Titre	Bulletin d'actualité 2012-24
Date de la première version	15 juin 2012
Date de la dernière version	–
Source	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

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

1 Paramètres dans l'URL : précautions nécessaires

Cette semaine, le CERTA a signalé à l'un de ses correspondants une vulnérabilité d'une application web permettant à un utilisateur de lire des informations concernant un autre utilisateur. Cette vulnérabilité ressurgit régulièrement. Il est donc utile de faire un rappel.

Le problème est simple. L'application est accessible de l'Internet, sans authentification. Chaque dossier contient des informations nominatives (nom, adresse...). L'URL contient un paramètre qui est le numéro de dossier, par exemple : `http://www.example.com/page.cgi?n=12345` . Ce numéro de dossier est séquentiel.

L'utilisateur dont le numéro de dossier est 12345 peut modifier celui-ci et accéder aux données relatives au dossier 12344, qui existe certainement, et 12346, qui risque d'exister si l'application a une utilisation élevée.

Si un paramètre est déterminant pour accéder à des enregistrements, ses valeurs possibles ne doivent pas être prévisibles. Ainsi, une numérotation aléatoire non séquentielle des dossiers aurait suffit à empêcher la recherche simple décrite ci-dessous. L'élargissement de l'espace des valeurs possibles rend les recherches exhaustives plus visibles ou moins rentables. La surveillance des échecs d'accès permet de détecter ces recherches exhaustives.

Par ailleurs, lorsque des données nominatives sont en jeu, il faut en protéger l'accès. Une authentification préalable est donc nécessaire.

2 Vulnérabilité dans les équipements *F5 BIG-IP*

Cette semaine, le CERTA a publié un avis sur une vulnérabilité présente dans les produits *F5 BIG-IP*. Cette vulnérabilité permet à un attaquant de se connecter sous le compte de *root* en utilisant SSH. Elle est due à une erreur de configuration d'origine du produit. Une clé publique est configurée pour que l'utilisateur *root* puisse se connecter en SSH, cependant la clé privée associée est présente et est la même sur tous les systèmes. Une personne en possession de cette dernière a donc la possibilité de se connecter sur n'importe quel équipement *F5 BIG-IP* vulnérable. Une preuve de concept avec la clé privée est disponible sur l'Internet.

Un correctif est disponible et doit être appliqué le plus rapidement possible (voir le lien vers l'avis du CERTA dans la partie *Documentation)*.

Il est également intéressant de noter que des bonnes pratiques peuvent limiter les risques d'exploitation de vulnérabilités de cette sorte :

- exposer l'interface d'administration uniquement sur des réseaux fiables ;
- mettre en place un filtrage au niveau réseau pour empêcher les accès non autorisés ;
- restreindre l'accès à SSH en configurant seulement des plages d'adresses IP autorisées.

Documentation

- Avis du CERTA concernant la vulnérabilité dans *F5 BIG-IP* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-313/index.html
- Bulletin de sécurité F5 :
  http://support.f5.com/kb/en-us/solutions/public/13000/600/sol13600.html

3 Mises à jour de sécurité dans Adobe

Le 8 juin l'éditeur *Adobe* a publié une suite de correctifs sur son produit *Flash Player*. Sept vulnérabilités ont été corrigées aussi bien sur *Windows* que *MacOS* et *Linux*. Six d'entre elles peuvent mener à une exécution de code arbitraire à distance, les plus critiques sont :

- CVE-2012-2034 et CVE-2012-2034 utilisant une compromission en mémoire ;
- CVE-2012-2035 utilisant un débordement de mémoire tampon dans la pile ;
- CVE-2012-2036 utilisant un débordement d'entier.

Le CERTA recommande d'appliquer les correctifs de l'éditeur dès que possible et selon la PSSI.

4 Mise à jour mensuelle Microsoft

Cette semaine, le CERTA a publié une alerte concernant XML Core Services. La vulnérabilité, mentionnée comme activement exploitée par Microsoft, permet l'exécution de code arbitraire à distance si un utilisateur visite une page Web spécialement conçue.

En attendant le correctif, le CERTA recommande d'utiliser des logiciels alternatifs ou d'appliquer les méthodes de contournement provisoires (cf. Alerte CERTA-2012-ALE-003 du 14 juin 2012).

Concernant la mise à jour mensuelle de Miscrosoft, sept bulletins ont été publiés dont trois sont considérés comme critiques.

Les vulnérabilités corrigées permettent :

- une exécution de code arbitraire à distance ;
- une élévation de privilèges.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Documentation

- Alerte CERTA-2012-ALE-003 du 14 juin 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-003/
- Synthèse des bulletins de sécurité Microsoft du mois de juin 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-jun

5 Rappel des avis émis

Dans la période du 08 au 14 juin 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-ALE-003 : Vulnérabilité dans Microsoft XML Core Services
- CERTA-2012-AVI-310 : Vulnérabilités dans PostgreSQL
- CERTA-2012-AVI-311 : Vulnérabilité dans Checkpoint IPSO
- CERTA-2012-AVI-312 : Vulnérabilités dans Adobe Flash Player et Adobe AIR
- CERTA-2012-AVI-313 : Vulnérabilité dans F5 BIG-IP et Enterprise Manager
- CERTA-2012-AVI-314 : Vulnérabilité dans MySQL et MariaDB
- CERTA-2012-AVI-315 : Vulnérabilité dans MantisBT
- CERTA-2012-AVI-316 : Multiples vulnérabilités dans HP Onboard Administrator
- CERTA-2012-AVI-317 : Vulnérabilité dans HP Web Jetadmin
- CERTA-2012-AVI-318 : Vulnérabilité dans Check Point Endpoint Connect
- CERTA-2012-AVI-319 : Vulnérabilité dans le noyau Linux
- CERTA-2012-AVI-320 : Vulnérabilité dans Windows Remote Desktop Protocol
- CERTA-2012-AVI-321 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2012-AVI-322 : Vulnérabilité dans NET Framework
- CERTA-2012-AVI-323 : Vulnérabilités dans Microsoft Lync
- CERTA-2012-AVI-324 : Vulnérabilité dans Microsoft Dynamics AX Enterprise Portal
- CERTA-2012-AVI-325 : Multiples vulnérabilités dans le noyau Windows (win32ksys)
- CERTA-2012-AVI-326 : Vulnérabilités dans le noyau Windows
- CERTA-2012-AVI-327 : Vulnérabilité dans Microsoft XML Core Services
- CERTA-2012-AVI-328 : Vulnérabilités dans Xen
- CERTA-2012-AVI-329 : Vulnérabilités dans iTunes
- CERTA-2012-AVI-330 : Vulnérabilité dans HP Server Automation
- CERTA-2012-AVI-331 : Multiples vulnérabilités dans Oracle Java
- CERTA-2012-AVI-332 : Multiples vulnérabilités dans Mac OS X
- CERTA-2012-AVI-333 : Vulnérabilités dans VMware

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

15 juin 2012 version initiale.