Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mars 2012
N° CERTA-2012-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-11

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-011

Gestion du document

Référence	CERTA-2012-ACT-011
Titre	Bulletin d'actualité 2012-11
Date de la première version	16 mars 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 Mises à jour de sécurité Microsoft

Mardi 14 mars 2012, Microsoft a diffusé, dans le cadre de ses correctifs mensuels, une liste de six avis de sécurité. Cette liste comporte deux bulletins particulièrement importants car ils concernent deux services réseau sensibles : RDP (*Remote Desktop Protocol* aussi appelé *Terminal Server*) et DNS.

1.1 Vulnérabilités RDP

Le bulletin *MS2012-020* concerne deux vulnérabilités du service RDP de Windows (CVE-2012-0002 et CVE-2012-0152), classées comme « Critique » par Microsoft. Elles permettent la prise de contrôle de la cible à distance. L'exploitation de ces failles pourrait être intégrée à un ver.

Le protocole RDP est couramment utilisé pour l'administration à distance des serveurs.
De plus, la fonction d'assistance à distance des postes utilisateur utilise également le protocole RDP. Cependant le service RDP est activé uniquement pendant la demande d'aide.

1.2 Vulnérabilité DNS

Le bulletin *MS12-017* concerne une vulnérabilité DNS de Windows (CVE-2012-0006), classée comme « Importante » par Microsoft. L'exploitation de cette vulnérabilité provoque un redémarrage de la machine. Cette action répétée peut fortement affecter un système d'information selon la criticité du serveur attaqué.

1.3 Recommandations

Le CERTA recommande le déploiement de ces mises à jour de sécurité. De plus, le filtrage en périphérie du port 3389/TCP est également conseillé.

Documentations

- CERTA-2012-AVI-135 : Vulnérabilité dans le DNS de Microsoft Windows
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-135
- CERTA-2012-AVI-136 : Vulnérabilité dans le noyau Microsoft Windows
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-136
- CERTA-2012-AVI-137 : Vulnérabilité dans Windows DirectWrite
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-137
- CERTA-2012-AVI-138 : Vulnérabilités dans Remote Desktop Protocol
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-138
- CERTA-2012-AVI-139 : Vulnérabilité dans Microsoft Visual Studio
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-139
- CERTA-2012-AVI-140 : Vulnérabilité dans Microsoft Expression Design
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-140

2 Mise à jour Cisco

Cisco Adaptive Security Appliances (ASA) propose une fonctionnalité connue sous le nom de *Cisco Clientless VPN Solution*. Elle permet aux utilisateurs de créer un tunnel SSL VPN via un navigateur Web. Au moment de la connexion, ASA transmet plusieurs contrôles ActiveX et applications Java au client. L'un de ces contrôles ActiveX *Cisco port forwarder* est affecté par une vulnérabilité (CVE-2012-0358) qui permet l'exécution de code arbitraire à distance, si l'utilisateur est par la suite incité à naviguer sur des pages Web spécialement conçues.

Cisco propose une mise à jour pour ASA qui corrige le contrôle ActiveX distribué. Néanmoins, les utilisateurs ayant déjà téléchargé ce contrôle ActiveX resteront vulnérables. Ces derniers doivent désactiver le contrôle ActiveX via une des méthodes proposées par Cisco dans son avis de sécurité.

Le CERTA a publié un avis concernant cette vulnérabilité (CERTA-2012-AVI-144).

Documentation

- Détails sur la vulnérabilité :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient
- Avis CERTA-2012-AVI-144 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-144

3 Rappel des avis émis

Dans la période du 09 au 15 mars 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-126 : Vulnérabilités dans iTunes
- CERTA-2012-AVI-127 : Vulnérabilités dans Apple iOS
- CERTA-2012-AVI-128 : Vulnérabilité dans Barracuda WAF
- CERTA-2012-AVI-129 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-130 : Vulnérabilité dans VMware vCenter Chargeback Manager
- CERTA-2012-AVI-131 : Vulnérabilité dans Splunk
- CERTA-2012-AVI-132 : Vulnérabilités dans Joomla!
- CERTA-2012-AVI-133 : Vulnérabilités dans les produits VMware
- CERTA-2012-AVI-134 : Vulnérabilités dans OpenSSL
- CERTA-2012-AVI-135 : Vulnérabilité dans le DNS de Microsoft Winndows
- CERTA-2012-AVI-136 : Vulnérabilité dans le noyau Microsoft Windows

– CERTA-2012-AVI-137 : Vulnérabilité dans Windows DirectWrite
– CERTA-2012-AVI-138 : Vulnérabilités dans Remote Desktop Protocol
– CERTA-2012-AVI-139 : Vulnérabilité dans Microsoft Visual Studio
– CERTA-2012-AVI-140 : Vulnérabilité dans Microsoft Expression Design
– CERTA-2012-AVI-141 : Vulnérabilités dans Safari
– CERTA-2012-AVI-142 : Vulnérabilités dans les produits Mozilla
– CERTA-2012-AVI-143 : Vulnérabilités dans McAfee EWS et MEG
– CERTA-2012-AVI-144 : Vulnérabilité dans Cisco ASA 5500
– CERTA-2012-AVI-145 : Vulnérabilité dans Adobe ColdFusion
– CERTA-2012-AVI-146 : Vulnérabilités dans HP Data Protector Express

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

– CERTA-2011-AVI-013-001 : Vulnérabilité dans sudo (ajout du bulletin de sécurité Gentoo)
– CERTA-2011-AVI-465-001 : Vulnérabilité dans stunnel (ajout du bulletin de sécurité Gentoo)
– CERTA-2012-AVI-028-002 : Vulnérabilité dans OpenSSL (ajout du bulletin de sécurité Gentoo)
– CERTA-2012-AVI-091-001 : Vulnérabilité dans libvorbis (ajout du bulletin de sécurité OpenSuse)
– CERTA-2012-AVI-094-002 : Vulnérabilité dans libxml2 (ajout du bulletin de sécurité Gentoo)
– CERTA-2012-AVI-115-001 : Vulnérabilités dans Adobe Flash Player (ajout du bulletin de sécurité RedHat)

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 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.

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 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.

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

Gestion détaillée du document

16 mars 2012 version initiale.