Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 16 novembre 2015
N° CERTFR-2015-ACT-046

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-046

1 - Protéger son site Internet contre des attaques informatiques

Plusieurs documents sont consultables sur les sites du CERT-FR et de l'ANSSI afin de protéger un site Internet contre des attaques d'origine informatique comme les dénis de service et les défigurations. Dans ce dernier cas, un site insuffisamment protégé pourrait être modifié à l'insu de son propriétaire afin de relayer une information de propagande et faire écho à un événement fortement médiatisé.

Il est rappelé que certaines mesures techniques simples peuvent être appliquées afin de limiter le succès d'une attaque de ce type :

- renouveler par un mot de passe durci les mots de passe des comptes privilégiés (administration, publication) ;
- sécuriser les accès d'administration et de publication des sites Internet et réseaux sociaux ;
- appliquer les derniers correctifs de sécurité du gestionnaire de contenu (CMS) utilisé ;
- augmenter le niveau de journalisation des serveurs et des équipements réseau.

Enfin, le CERT-FR recommande de ne pas suivre un lien ou ouvrir la pièce jointe d'un courriel non sollicité (message incohérent, expéditeur inconnu, objet du message suspicieux, etc.). Il convient également d'alerter le responsable sécurité informatique de l'entité en cas de doute sur un message.

Documentation

- http://www.ssi.gouv.fr/fr/menu/actualites/proteger-son-site-internet-des-cyberattaques.html
- http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html

2 - Gestion des mots de passe des administrateurs locaux

Introduction

Le CERT-FR constate régulièrement l'utilisation des GPO de préférence (ou GPP pour Group Policy Preferences) pour gérer les comptes locaux des postes de travail ou des serveurs Windows. Cette méthode est désormais déconseillée et doit être remplacée par LAPS (Local Administrator Password Solution). Ce bulletin, en deux parties, détaille dans une première partie la faiblesse du stockage des mots de passe dans les GPO de préférence et, dans une deuxième partie, le mécanisme LAPS.

GPP

Parmi les fonctionnalités offertes par les GPO de préférence, l'une d'entre elles permet la création d'objets sur le système sur lequel une GPO de ce type est appliquée. Parmi ces objets, plusieurs d'entre eux ont la particularité d'enregistrer un mot de passe associé à l'objet crée :

- utilisateur local ;

– tâche planifiée ;
– service Windows ;
– mappage de lecteur réseau ;
– source de données ODBC.

Ainsi, tous les mots de passe stockés dans les GPO de préférence sont encodés puis positionnés dans un attribut dénommé `cpassword`. Cet attribut est présent dans les fichiers XML définissant les GPO de préférence (Groups.xml, ScheduledTasks.xml, Services.xml, DataSources.xml et Drives.xml). Cet encodage est facilement réversible et publiquement documenté par Microsoft. Les fichiers XML de définition des GPO de préférence sont stockés sur le partage SYSVOL qui est, par défaut, accessible à tous les utilisateurs authentifiés membres d'un domaine Active Directory. Dans une telle situation, il devient possible, pour des utilisateurs sans droit particulier, de récupérer les fichiers XML puis de décoder les mots de passe stockés. Des outils réalisant ces opérations sont publiquement disponibles.

En mai 2014, Microsoft a publié un bulletin le sécurité MS14-025 detaillant la faiblesse du stockage des mots de passe mis en œuvre dans les GPO de préférence et corrigeant le problème. Il faut cependant noter que le correctif ne modifie pas la façon dont les mots de passe sont encodés, mais se contente d'interdire, via les interfaces graphiques, le stockage de nouveaux mots de passe. Ainsi, la configuration n'est pas modifiée et les mots de passe déjà stockés ne sont pas supprimés.
Le KB2962486 fournit en complément un script Powershell permettant d'identifier, dans toutes les GPO, la présence d'attribut `cpassword`. Le CERT-FR recommande donc l'appliquer le correctif et de supprimer tous les mots passe encodés.

Ceci peut cependant constituer une perte de fonctionnalité, en particulier pour la gestion des comptes locaux. Le deuxième bulletin détaillera le mécanisme LAPS qui permet de gérer de manière sécurisée les mots de passe des comptes locaux des systèmes Windows.

Documentation

– http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
– https://support.microsoft.com/en-us/kb/2962486

3 - Mise à jour mensuelle de Microsoft

Le 10 novembre 2015, Microsoft a publié douze bulletins de sécurité, dont cinq sont considérés comme critiques et sept comme importants :

– MS15-112 (critique) qui concerne Internet Explorer ;
– MS15-113 (critique) qui concerne Edge ;
– MS15-114 (critique) qui concerne Windows Journal ;
– MS15-115 (critique) qui concerne le noyau de Windows ;
– MS15-116 (critique) qui concerne Microsoft Office ;
– MS15-117 (important) qui concerne NDIS ;
– MS15-118 (important) qui concerne .NET ;
– MS15-119 (important) qui concerne Winsock ;
– MS15-120 (important) qui concerne IPSec ;
– MS15-121 (important) qui concerne Schannel ;
– MS15-122 (important) qui concerne Kerberos ;
– MS15-123 (important) qui concerne Skype et Microsoft Lync.

Navigateurs

Les navigateurs de Microsoft, Internet Explorer et Edge, font tous les deux l'objet de bulletins. La mise à jour d'Internet Explorer (bulletin MS15-112) corrige vingt-six vulnérabilités qui peuvent conduire à une exécution de code à distance. Concernant Microsoft Edge (bulletin MS15-113), quatre vulnérabilités sont corrigées qui peuvent également conduire à une exécution de code à distance ou à un contournement de mécanismes de sécurité tels que la disposition aléatoire de l'espace d'adressage. Une élévation de privilèges a également été corrigée dans le framework .NET via le bulletin MS15-118. Un attaquant pourrait l'exploiter en incitant l'utilisateur à accéder à un site web compromis afin d'injecter du code dans le navigateur.

Windows

Le bulletin MS15-114 corrige quant à lui une vulnérabilité dans Windows. Cette vulnérabilité concerne la gestion de fichiers de type Journaux. Elle peut conduire à une exécution de code arbitraire à distance. Le noyau Windows est également ciblé par un bulletin de sécurité (bulletin MS15-115). Sept vulnérabilités sont corrigées permettant une exécution de code à distance, une élévation de privilèges ou une fuite d'information. Une vulnérabilité a été corrigée dans Microsoft Windows NDIS grâce au bulletin MS15-117. Elle permet à un attaquant de provoquer une élévation de privilèges. Le bulletin MS15-119 corrige une élévation de privilèges dans Windows Winsock. Le service IPSec de Windows est également sujet à une correction pour la vulnérabilité CVE-2015-6111 (bulletin MS15-120) qui permet un déni de service. La vulnérabilité CVE-2015-6112 est corrigée dans le bulletin MS15-121 et impacte la gestion du protocole TLS de Microsoft Windows. Un attaquant en situation d'homme du milieu pourrait l'exploiter afin d'usurper l'identité d'une victime sur un autre serveur. La vulnérabilité CVE-2015-6095 impactant le protocole Kerberos est corrigée dans le bulletin MS15-122. Cette vulnérabilité permet de contourner le mécanisme d'authentification et de déchiffrer un lecteur protégé par BitLocker.

Bureautique

Le bulletin MS15-116 fait état de sept vulnérabilités. Ces vulnérabilités pourraient permettre l'exécution de code à distance si un utilisateur venait à ouvrir un fichier Microsoft Office spécialement conçu. Cela concerne plusieurs versions de Microsoft Office, de la version 2007 à la version 2013 ainsi que les serveurs SharePoint 2010 et 2013.

Enfin, la vulnérabilité CVE-2015-6061 impactant Skype est corrigée dans le bulletin MS15-123. Un attaquant pourrait l'exploiter via un code JavaScript spécialement formé en incitant sa victime à entreprendre une conversation instantanée.

Documentation

- https://technet.microsoft.com/en-us/library/security/MS15-112
- https://technet.microsoft.com/en-us/library/security/MS15-113
- https://technet.microsoft.com/en-us/library/security/MS15-114
- https://technet.microsoft.com/en-us/library/security/MS15-115
- https://technet.microsoft.com/en-us/library/security/MS15-116
- https://technet.microsoft.com/en-us/library/security/MS15-117
- https://technet.microsoft.com/en-us/library/security/MS15-118
- https://technet.microsoft.com/en-us/library/security/MS15-119
- https://technet.microsoft.com/en-us/library/security/MS15-120
- https://technet.microsoft.com/en-us/library/security/MS15-121
- https://technet.microsoft.com/en-us/library/security/MS15-122
- https://technet.microsoft.com/en-us/library/security/MS15-123

4 - Rappel des avis émis

Dans la période du 09 au 15 novembre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-465 : Multiples vulnérabilités dans Cisco AsyncOS
- CERTFR-2015-AVI-466 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2015-AVI-467 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2015-AVI-468 : Vulnérabilité dans Cisco Connected Grid Network Management
- CERTFR-2015-AVI-469 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-470 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2015-AVI-471 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-472 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2015-AVI-473 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-474 : Vulnérabilité dans Microsoft Windows

- CERTFR-2015-AVI-475 : Multiples vulnérabilités dans Microsoft .NET Framework
- CERTFR-2015-AVI-476 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-477 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-478 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-479 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-480 : Vulnérabilité dans Microsoft Skype
- CERTFR-2015-AVI-481 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-482 : Vulnérabilité dans Google Chrome
- CERTFR-2015-AVI-483 : Vulnérabilité dans Cisco FireSIGHT Management Center
- CERTFR-2015-AVI-484 : Multiples vulnérabilités dans Oracle WebLogic Server
- CERTFR-2015-AVI-485 : Multiples vulnérabilités dans Citrix NetScaler Service Delivery Appliance
- CERTFR-2015-AVI-486 : Vulnérabilité dans Cisco IOS
- CERTFR-2015-AVI-487 : Vulnérabilité dans Huawei P7

Gestion détaillée du document

16 novembre 2015 version initiale.