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 février 2015
N° CERTFR-2015-ACT-007

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-007

1 - Mise à jour mensuelle Microsoft

Lors de sa mise à jour mensuelle du 10 février 2015, Microsoft a publié 9 bulletins de sécurité, dont trois sont considérés comme critiques et 6 comme importants :

- MS15-009 (Critique) qui concerne Internet Explorer ;
- MS15-010 (Critique) qui concerne le pilote en mode noyau de Windows ;
- MS15-011 (Critique) qui concerne la stratégie de groupe de Windows ;
- MS15-012 (Important) qui concerne Microsoft Office ;
- MS15-013 (Important) qui concerne Microsoft Office ;
- MS15-014 (Important) qui concerne la stratégie de groupe de Windows ;
- MS15-015 (Important) qui concerne Microsoft Windows ;
- MS15-016 (Important) qui concerne le composant graphique de Windows ;
- MS15-017 (Important) qui concerne Virtual Machine Manager.

La mise à jour MS15-009 corrige 41 vulnérabilités dans Internet Explorer. Elle corrige en particulier 35 vulnérabilités de type corruption de mémoire, dont certaines touchent toutes les versions d'Internet Explorer (6 à 11). La plupart de ces vulnérabilités permettent une exécution de code arbitraire à distance. Par ailleurs, ce correctif corrige deux élévations de privilèges, trois contournements de la distribution aléatoire de l'espace mémoire et une fuite d'informations interdomaines.

Le correctif MS15-010, considéré comme critique, corrige deux vulnérabilités de type exécution arbitraire de code à distance, un déni de service et deux élévations de privilèges dans le pilote win32k.sys. Cette mise à jour corrige également un contournement de sécurité dans le pilote cng.sys. Cette vulnérabilité avait été révélée publiquement le 15 janvier 2015.

Le correctif MS15-011, considéré lui aussi comme critique, corrige une vulnérabilité dans l'application des stratégies de groupe (GPO) permettant une exécution de code arbitraire à distance. Microsoft recommande par ailleurs d'activer la nouvelle fonctionnalité dite UNC Hardened Access pour se protéger contre cette attaque. La documentation en annexe fournit de plus amples informations sur cette procédure.

Les correctifs MS15-012 et MS15-013 corrigent quatre vulnérabilités dans Microsoft Office. Trois de ces vulnérabilités concernent une exécution de code à distance, et une, révélée publiquement, permet un contournement de la fonctionnalité de distribution aléatoire de l'espace mémoire. Les autres correctifs, considérés comme importants, corrigent deux vulnérabilités permettant une élévation de privilèges, une vulnérabilité permettant un contournement de sécurité dans les stratégies de groupe (GPO) et une vulnérabilité dans le composant graphique de Windows.

Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande de les appliquer dès que possible.

Documentation

- https://technet.microsoft.com/fr-fr/library/security/MS15-009
- https://technet.microsoft.com/fr-fr/library/security/MS15-010
- https://technet.microsoft.com/fr-fr/library/security/MS15-011
- https://technet.microsoft.com/fr-fr/library/security/MS15-012
- https://technet.microsoft.com/fr-fr/library/security/MS15-013
- https://technet.microsoft.com/fr-fr/library/security/MS15-014
- https://technet.microsoft.com/fr-fr/library/security/MS15-015
- https://technet.microsoft.com/fr-fr/library/security/MS15-016
- https://technet.microsoft.com/fr-fr/library/security/MS15-017
- https://support.microsoft.com/kb/3000483

2 - Formulaires de contact

Certains sites Internet souhaitent masquer l'adresse de messagerie permettant de contacter les administrateurs. Elle est remplacée par un ou plusieurs formulaires de contact. Un attaquant peut cependant tenter d'automatiser la validation du formulaire afin d'émettre des courriels indésirables ou malveillants aux équipes en charge de la gestion du site.

Protections

Il convient tout d'abord de suivre les bonnes pratiques d'implémentation d'un formulaire sur un site internet. Certains codes de formulaires demandent de renseigner l'adresse de contact dans un champ du code HTML de la page Web. Elle est donc visible par le navigateur, ce qui annule l'intérêt du formulaire et permet à un attaquant de viser directement cette adresse.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Des bibliothèques de type « CAPTCHA » vont permettre au développeur Web de forcer le visiteur du formulaire à résoudre un problème simple qui devra être validé pour que l'email soit émis.

Ce problème doit être facilement traité par un être humain, mais coûteux en ressources pour une machine. Il s'agit de dissuader un attaquant en s'assurant que le coût de résolution du problème soit plus élevé que le gain de l'envoi d'un spam.

Parmis ces problèmes, plusieurs exemples peuvent être implémentés:

- répondre à une question simple ;
- résoudre un calcul simple posé textuellement (ex: « indiquer en chiffres la somme de trois et de sept ») ;
- transcrire le contenu d'une image contenant des caractères déformés ;
- reconnaître des formes ou des objets dans une image ;
- etc.

Toutefois, des chercheurs ont pu déjouer les algorithmes de génération des problèmes de certaines bibliothèques. Un autre inconvénient de certaines implémentations de CAPTCHA est qu'elles empêchent souvent l'utilisation du formulaire aux personnes déficientes visuelles. Il convient ainsi de vérifier qu'un problème visuel pourra être changé en problème énoncé de manière sonore.

Les versions les plus avancées sont capables de détecter la manière dont l'utilisateur répond au problème (mouvements de la souris, durée de validation du formulaire, etc.) afin de déterminer si le visiteur est une personne ou un robot.

En-tête « HTTP_REFERER »

Le code de validation du formulaire pourra vérifier la valeur de l'en-tête « HTTP_REFERER ». Celle-ci indiquera si le visiteur a effectivement navigué sur le site avant d'envoyer le formulaire. Cette variable peut toutefois être positionnée correctement par un script d'envoi de mail automatique.

Ajout de champs cachés

Cette solution consiste à mettre en place un champ caché dans le formulaire et de contrôler sa valeur par script. Partant du principe qu'un robot tentera de remplir tous les champs, il pourra modifier autant les champs visibles que les champs cachés. Il suffira de vérifier si un des champs cachés est renseigné, cela signifiera qu'un robot est à l'origine de la saisie.

A prendre en considération : malgré l'option `display:none` activée, il peut arriver que ce champ reste visible. Dans cette éventualité, il est recommandé d'utiliser un libellé explicite (« ne remplissez pas ce champ »), afin que le visiteur laisse ce champ vierge.

Il est également possible aux codes automatisant l'envoi de formulaire, de vérifier si ces champs sont visibles ou non.

Nommer les champs de saisie aléatoirement

Les robots se basent sur une liste de mots clefs afin d'identifier les champs: Nom / name / mail / e-mail /email , etc. Nommer ces champs avec des noms différents, voir aléatoirement (tout en conservant une table de correspondance), peut perturber le fonctionnement de scripts automatisés.

Validation par mail

Après saisie, un message comportant un lien de validation est envoyé immédiatement à l'auteur, par l'intermédiaire de l'adresse mail spécifiée. Le message n'est considéré comme étant effectivement envoyé qu'après un clic de l'auteur sur ce lien.

Pour conclure, la plupart des solutions peuvent être contournées par des automates de pourriels. L'utilisation de plusieurs mesures parmi celles citées, permettra de limiter l'exploitation abusive du formulaire, tout en sachant qu'il ne sera jamais complètement invulnérable. La mise en place de dispositifs antispam est recommandée pour filtrer les courriels indésirables.

Documentation

- Bibliothèque ReCaptcha :
  https://developers.google.com/recaptcha/
- Recommandations pour la sécurisation des sites Web :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf

3 - Rappel des avis émis

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

- CERTFR-2015-ALE-004 : Vulnérabilité dans Microsoft Internet Explorer
- CERTFR-2015-AVI-060 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-061 : Multiples vulnérabilités dans le pilote en mode noyau de Microsoft Windows
- CERTFR-2015-AVI-062 : Vulnérabilité dans la stratégie de groupe (GPO) de Microsoft Windows
- CERTFR-2015-AVI-063 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-064 : Vulnérabilité dans Microsoft Office
- CERTFR-2015-AVI-065 : Vulnérabilité dans la stratégie de groupe (GPO) de Microsoft Windows
- CERTFR-2015-AVI-066 : Vulnérabilité dans Microsoft Windows
- CERTFR-2015-AVI-067 : Multiples vulnérabilités dans le composant Microsoft Graphics de Microsoft Windows
- CERTFR-2015-AVI-068 : Vulnérabilité dans Microsoft Virtual Machine Manager
- CERTFR-2015-AVI-069 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-070 : Multiples vulnérabilités dans PostgreSQL
- CERTFR-2015-AVI-071 : Vulnérabilité dans les produits F5 BIG-IP

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

- CERTFR-2015-AVI-059 : Vulnérabilité dans Moodle (version initiale.)

Gestion détaillée du document

16 février 2015 version initiale.