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 14 août 2014
N° CERTFR-2014-ACT-033

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-033

1 - Vulnérabilités touchant Windows XP

Des vulnérabilités dans des modules noyaux (drivers) de Windows XP ont récemment été publiées sur Internet. Elles permettent de provoquer une écriture arbitraire dans l'espace noyau. Ces vulnérabilités peuvent mener un utilisateur maveillant à élever son niveau de privilèges sur le système. D'autres failles similaires, éventuellement plus graves encore, feront probablement leur apparition dans le futur. Le CERT-FR rappelle que Microsoft a cessé le support technique de Windows XP en avril 2014. De ce fait aucun correctif ne sera mis à disposition par Microsoft pour Windows XP.

Recommandations

Le CERT-FR recommande de migrer au plus tôt les systèmes d'exploitation obsolètes non maintenus par leur éditeur, vers des systèmes maintenus pour pouvoir bénéficier des derniers correctifs de sécurité. Il est également recommandé de ne pas utiliser de méthode permettant de contourner les restrictions mises en place au niveau du service de mise à jour et de ne pas chercher à recevoir des correctifs dédiés à une autre version du système d'exploitation. De plus, le CERT-FR alerte les utilisateurs sur le potentiel danger lié à la publication de faux correctifs pour des logiciels qui ne sont plus supportés par leur éditeur. En effet, des personnes malintentionnées peuvent être tentées de diffuser des codes malveillants en les faisant passer pour des correctifs. Dans ce cadre, le CERT-FR attire l'attention sur le fait qu'il est important de n'appliquer que des correctifs officiels publiés par l'éditeur.

Documentation

http://www.ssi.gouv.fr/fr/menu/actualites/arret-du-support-de-windows-xp-recommandations.html

2 - Publication Appel à commentaires sur le référentiel d'exigences cloud

Le 11 août 2014, l'ANSSI a publié un appel public à commentaires sur un référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage.

Le référentiel de qualification de prestataires propose une offre de services en nuage qui recouvre les offres de type SaaS, PaaS et IaaS. Il se décline selon deux niveaux de sécurité :

- le niveau élémentaire, qui correspond aux exigences portées par la PSSIE ;
- le niveau standard, correpondant à une protection accrue, qui vise le traitement des données de niveau «_Diffusion Restreinte_».

Les exigences, relatives aux prestataires, sont déclinées en quatorze chapitres et portent notamment sur le contrôle d'accès et la gestion des identités, la sécurité liée à l'exploitation, et la gestion des incidents liés à la

sécurité de l'information. Ces exigences seront vérifiées au travers d'un audit des lieux liés à la prestation visée par la qualification.

Les observations, commentaires et propositions peuvent être transmis d'ici lundi 3 novembre 2014.

Documentation

Appel à commentaires sur la publication du référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage :
http://www.ssi.gouv.fr/fr/menu/actualites/appel-commentaires-referentiel-d-exigences-informatique-nuage.html

3 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié neuf bulletins de sécurité, dont deux considérés comme critiques et sept comme importants :

- MS14-043 (critique) qui concerne Windows Media Player ;
- MS14-044 (important) qui concerne SQL Server ;
- MS14-045 (important) qui concerne le noyau de Windows ;
- MS14-046 (important) qui concerne .NET ;
- MS14-047 (important) qui concerne le mécanisme LRPC de Windows ;
- MS14-048 (important) qui concerne OneNote ;
- MS14-049 (important) qui concerne Windows Installer ;
- MS14-050 (important) qui concerne SharePoint Server ;
- MS14-051 (critique) qui concerne Internet Explorer.

La vulnérabilité dans Windows Media Player est de type use-after-free et pourrait être exploitée en persuadant un utilisateur d'ouvrir un document Microsoft Office malveillant. La majorité des vingt-six vulnérabilités corrigées dans Internet Explorer sont des corruptions mémoire susceptibles de conduire à de l'exécution de code arbitraire à distance. À ce jour, au moins l'une d'entre elles (CVE-2014-2817) est activement exploitée dans des attaques ciblées. Certaines des vulnérabilités importantes corrigées ce mois-ci, notamment celles situées dans le pilote win32k.sys (MS14-045), permettent une élévation de privilèges. D'autres permettent de contourner le mécanisme d'ASLR (MS14-046, MS14-047). Le CERT-FR recommande l'application des correctifs de sécurité dès que possible.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-345/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-346/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-347/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-348/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-349/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-350/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-351/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-352/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-353/index.html

4 - Rappel des avis émis

Dans la période du 08 au 13 août 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-345 : Vulnérabilité dans Microsoft Windows Media Player
- CERTFR-2014-AVI-346 : Multiples vulnérabilités dans Microsoft SQL Server
- CERTFR-2014-AVI-347 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2014-AVI-348 : Vulnérabilité dans Microsoft .NET
- CERTFR-2014-AVI-349 : Vulnérabilité dans Microsoft Windows LRPC
- CERTFR-2014-AVI-350 : Vulnérabilité dans Microsoft OneNote

- CERTFR-2014-AVI-351 : Vulnérabilité dans Microsoft Windows Installer
- CERTFR-2014-AVI-352 : Vulnérabilité dans Microsoft SharePoint Server
- CERTFR-2014-AVI-353 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-354 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-355 : Multiples vulnérabilités dans Google Chrome

Gestion détaillée du document

14 août 2014 version initiale.