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 18 mai 2015
N° CERTFR-2015-ACT-020

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-020

1 - Incidents BGP

Chacun des acteurs de l'Internet (FAI, hébergeurs, diffuseurs de contenu, etc.) gère des blocs d'adresses IP contiguës. Afin de constituer l'infrastructure de l'Internet, les acteurs s'interconnectent entre eux à l'aide du protocole BGP (« `Border Gateway Protocol` »). L'objectif de ce protocole est d'échanger des informations de routage entre ces réseaux et de permettre les échanges entres ces différents acteurs.

La sécurité informatique n'était pas une préoccupation importante lors de la création de ce protocole, c'est la raison pour laquelle il intègre peu de mesures de sécurité. Il est ainsi possible pour n'importe quel acteur d'annoncer des adresses IP n'étant pas sous sa responsabilité, et ainsi réaliser des usurpations d'adresses IP. Les motivations derrière ces usurpations sont diverses et peuvent aller de l'envoi de courriels non sollicité, au détournement et à l'interception de trafic.

L'authenticité des interlocuteurs n'étant pas garantie par le protocole de transport IP, il est recommandé d'assurer un chiffrement de bout en bout pour toutes les communications sensibles qui transitent sur Internet, dès lors que cela est possible.

De plus, afin de détecter au plus tôt d'éventuelles usurpations, les administrateurs en charge de systèmes autonomes (« AS ») peuvent surveiller leurs préfixes d'adresses d'IP.

L'ANSSI, via l'Observatoire de la résilience de l'Internet français [1], observe les comportements des acteurs, et publie chaque année un rapport sur la résilience de l'Internet en France en analysant des données BGP et DNS. Si vous êtes victime d'une usurpation de vos préfixes IP, communiquez les informations relatives à cette usurpation (préfixe, numéro d'AS, numéro d'AS usurpateur) au CERT-FR.

Documentation

1 http://www.ssi.gouv.fr/observatoire
2 Bonnes pratiques de configuration de BGP:
http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf

2 - Mise à jour mensuelle de Microsoft

Lors de sa mise à jour mensuelle du 12 mai 2015, Microsoft a publié treize bulletins de sécurité, dont les trois premiers sont considérés comme critiques, et les autres comme importants :

- MS15-043 (critique) qui concerne Internet Explorer ;
- MS15-044 (critique) qui concerne la gestion des polices de caractères par Windows ;
- MS15-045 (critique) qui concerne l'application Windows Journal ;
- MS15-046 (important) qui concerne Microsoft Office ;
- MS15-047 (important) qui concerne SharePoint ;
- MS15-048 (important) qui concerne .NET ;

– MS15-049 (important) qui concerne Silverlight ;
– MS15-050 (important) qui concerne le gestionnaire de contrôle des services (SCM) de Windows ;
– MS15-051 (important) qui concerne le noyau de Windows ;
– MS15-052 (important) qui concerne le noyau de Windows ;
– MS15-053 (important) qui concerne les moteurs JScript et VBScript ;
– MS15-054 (important) qui concerne la console de gestion (MMC) de Windows ;
– MS15-055 (important) qui concerne la bibliothèque Schannel de Windows.

Le bulletin cumulatif MS15-043, concernant Internet Explorer, fait état de multiples corruptions mémoire pouvant entraîner une exécution de code arbitraire à distance, ainsi que de vulnérabilités permettant une élévation de privilèges, ou permettant le contournement du mécanisme d'ASLR (*Address Space Layout Randomization* - la distribution aléatoire de l'espace mémoire.)

Le bulletin MS15-044 corrige deux vulnérabilités dans la bibliothèque Windows DirectWrite de gestion des polices de caractères *OpenType* et *TrueType*, les CVE-2015-1670 et CVE-2015-1671. La première permet une atteinte à la confidentialité des données, la seconde, beaucoup plus sérieuse, permet une exécution de code arbitraire à distance sur un très grand nombre de plateformes et produits Microsoft : toutes les versions supportées de Windows, le *framework* .NET, Office, Live Meeting, Lync, et Silverlight.

Le bulletin MS15-045 corrige six vulnérabilités dans l'application de prise de notes Windows Journal. L'exploitation de ces vulnérabilités, liées au traitement des fichiers `.jnt`, pourrait permettre une exécution de code arbitraire à distance.

Deux vulnérabilités liées au traitement des fichiers Microsoft Office, susceptibles de permettre une exécution de code arbitraire par le biais de documents malformés, sont corrigées dans le bulletin MS15-046.

Le bulletin MS15-047, concernant Sharepoint, corrige des vulnérabilités dans le traitement des pages en provenance des clients, qui pourraient permettre à un attaquant de prendre le contrôle du processus W3WP sur le serveur Sharepoint, en lui soumettant des pages malformées.

Le bulletin MS15-048 concerne le *Framework* .NET et corrige deux vulnérabilités, dont l'une permettrait à un attaquant d'effectuer un déni de service à distance sur un site Web fondé sur .NET, et l'autre pourrait engendrer une élévation de privilèges.

La vulnérabilité dans Silverlight corrigée par le bulletin MS15-049 est de type "élévation de privilèges d'intégrité faible à intégrité intermédiaire", dans le cadre d'une application Silverlight tournant sous un navigateur. Elle pourrait permettre à un attaquant de sortir du cadre restreint d'un processus de faible intégrité, et d'effectuer toute action autorisée à l'utilisateur courant.

Le bulletin MS15-050 corrige une vulnérabilité dans le traitement des rôles utilisateurs (*impersonation levels*) par le gestionnaire de contrôle des services de Windows (*Service Control Manager*), qui pourrait permettre une élévation de privilèges.

Le bulletin MS15-051 corrige un ensemble de vulnérabilités dans le noyau de Windows permettant de faire fuiter le contenu de zones mémoire noyau vers le mode utilisateur, ce qui pourrait permettre à un attaquant, par exemple, de contourner le mécanisme d'ASLR, ainsi qu'une vulnérabilité du pilote win32k qui permet une élévation de privilèges en mode noyau.

Une fuite d'adresse mémoire, permettant elle aussi le contournement de l'ASLR du noyau, est corrigée dans le pilote cng.sys par le bulletin MS15-052.

Deux vulnérabilités permettant de contourner l'ASLR utilisateur sont corrigées dans les moteurs de script JScript et VBScript par le bulletin MS15-043.

Le bulletin MS15-044 corrige une vulnérabilité dans la console de gestion de Windows (*Microsoft Management Console*), liée au traitement des fichiers `.msc`, et permettant à un attaquant de provoquer un déni de service.

Enfin le bulletin MS15-045 corrige une vulnérabilité dans la bibliothèque de sécurisation des communications Schannel, qui pourrait permettre une atteinte à la confidentialité des données échangées lors d'une session TLS employant une clé trop faible.

Le CERT-FR recommande d'appliquer les correctifs mentionnés dans les plus brefs délais.

Documentation

– https://technet.microsoft.com/en-us/library/security/MS15-043
– https://technet.microsoft.com/en-us/library/security/MS15-044
– https://technet.microsoft.com/en-us/library/security/MS15-045

- https://technet.microsoft.com/en-us/library/security/MS15-046
- https://technet.microsoft.com/en-us/library/security/MS15-047
- https://technet.microsoft.com/en-us/library/security/MS15-048
- https://technet.microsoft.com/en-us/library/security/MS15-049
- https://technet.microsoft.com/en-us/library/security/MS15-050
- https://technet.microsoft.com/en-us/library/security/MS15-051
- https://technet.microsoft.com/en-us/library/security/MS15-052
- https://technet.microsoft.com/en-us/library/security/MS15-053
- https://technet.microsoft.com/en-us/library/security/MS15-054
- https://technet.microsoft.com/en-us/library/security/MS15-055

3 - Rappel des avis émis

Dans la période du 11 au 16 mai 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-207 : Multiples vulnérabilités dans WordPress
- CERTFR-2015-AVI-208 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-209 : Multiples vulnérabilités dans les pilotes de police de Microsoft Windows
- CERTFR-2015-AVI-210 : Multiples vulnérabilités dans Microsoft Windows Journal
- CERTFR-2015-AVI-211 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-212 : Vulnérabilité dans Microsoft SharePoint Server
- CERTFR-2015-AVI-213 : Multiples vulnérabilités dans Microsoft .NET
- CERTFR-2015-AVI-214 : Vulnérabilité dans Microsoft Silverlight
- CERTFR-2015-AVI-215 : Vulnérabilité dans le gestionnaire de contrôle des services de Microsoft Windows
- CERTFR-2015-AVI-216 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2015-AVI-217 : Vulnérabilité dans le noyau de Microsoft Windows
- CERTFR-2015-AVI-218 : Multiples vulnérabilités dans les composants JScript et VBscript de Microsoft Windows
- CERTFR-2015-AVI-219 : Vulnérabilité dans la console de gestion de Microsoft Windows
- CERTFR-2015-AVI-220 : Vulnérabilité dans la bibliothèque Schannel de Microsoft Windows
- CERTFR-2015-AVI-221 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2015-AVI-222 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-223 : Multiples vulnérabilités dans Wireshark
- CERTFR-2015-AVI-224 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-225 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-226 : Multiples vulnérabilités dans PHPMyAdmin
- CERTFR-2015-AVI-227 : Multiples vulnérabilités dans Adobe Reader et Acrobat

Gestion détaillée du document

18 mai 2015 version initiale.