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 19 janvier 2015
N° CERTFR-2015-ACT-003

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-003

1 - Mise à jour mensuelle Microsoft

Lors de sa mise à jour mensuelle du 13 janvier 2015, Microsoft a publié huit bulletins de sécurité, dont un est considéré comme critique :

- MS15-001 (important) : cache AppCompat de Windows ;
- MS15-002 (critique) : service Telnet de Windows ;
- MS15-003 (important) : service de profil utilisateur de Windows ;
- MS15-004 (important) : composant TS WebProxy de Windows ;
- MS15-005 (important) : service NLA de Windows ;
- MS15-006 (important) : rapport d'erreurs de Windows ;
- MS15-007 (important) : serveur de stratégie réseau de Windows ;
- MS15-008 (important) : pilote WebDAV de Windows.

Les vulnérabilités MS15-001 et MS15-003, qui permettent une élévation de privilège, ont fait l'objet de débats dans la communauté de la sécurité informatique en raison de leur révélation précoce. En vertu de sa convention habituelle de divulgation, Google a révélé publiquement ces deux vulnérabilités 90 jours après en avoir notifié Microsoft, avant qu'un correctif ne soit disponible. Ces vulnérabilités sont donc désormais corrigées.

La vulnérabilité critique MS15-002 est un dépassement de tampon sur la pile dans le service Telnet permettant, en théorie, une exécution de code arbitraire à distance. Le service Telnet est désactivé par défaut dans toutes les versions supportées de Windows.

La vulnérabilité MS15-004 peut permettre à un attaquant de s'évader de la protection de type *sandbox* d'Internet Explorer. Microsoft indique que cette vulnérabilité a déjà été exploitée dans le cadre d'attaques, à faible échelle.

La vulnérabilité MS15-005 permet à un attaquant de simuler la présence d'un réseau local pour réduire la fonctionnalité du pare-feu d'une machine connectée à Internet.

La vulnérabilité MS15-006 dans la fonctionnalité de rapport d'erreurs de Windows pourrait être employée pour accéder à la mémoire d'un processus protégé.

La vulnérabilité MS15-007 pourrait permettre un déni de service à distance de l'authentification RADIUS.

Enfin, l'exploitation de la vulnérabilité MS15-008, présente dans le pilote noyau `mrxdav.sys` lié au protocole WebDAV, peut aboutir à une élévation de privilège.

Documentation

- https://technet.microsoft.com/en-us/library/security/MS15-001
- https://technet.microsoft.com/en-us/library/security/MS15-002
- https://technet.microsoft.com/en-us/library/security/MS15-003
- https://technet.microsoft.com/en-us/library/security/MS15-004

– https://technet.microsoft.com/en-us/library/security/MS15-005
– https://technet.microsoft.com/en-us/library/security/MS15-006
– https://technet.microsoft.com/en-us/library/security/MS15-007
– https://technet.microsoft.com/en-us/library/security/MS15-008

2 - Publication de deux fiches concernant la protection des site internet contre les cyberattaques

Depuis le 7 Janvier 2015, plusieurs groupes d'attaquants appellent à attaquer des sites institutionnels Français. Ces attaques se traduisent le plus souvent par des défigurations de sites web et des attaques en déni de service sur des serveurs. L'ANSSI a publié deux fiches rappelant différentes recommandations pour se protéger de ces types d'attaques.

La fiche de bonnes pratiques en cybersécurité rappelle les recommandations d'hygiène informatique pour se protéger de menaces génériques et présente des recommandations sur l'usage des réseaux sociaux. La fiche d'information pour les administrateurs présente les bonnes pratiques en matière de protection des sites contre les défigurations (comme la mise à jour des gestionnaires de contenu, ou « CMS ») et les attaques par déni de service (comme la souscription à des services de filtrage proposés par les fournisseurs de trafic).

Le CERT-FR encourage toutes les entités à appliquer au plus tôt les recommandations présentées dans ces fiches. En cas de compromission, le CERT-FR recommande de prendre immédiatement contact avec la chaîne de remontée des incidents de sécurité informatique (DSI, RSSI) de votre entité.

Documentation

– http://www.ssi.gouv.fr/IMG/pdf/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf
– http://www.ssi.gouv.fr/IMG/pdf/Fiche_d_information_Administrateurs.pdf
– http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
– http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf

3 - Rappel des avis émis

Dans la période du 12 au 18 janvier 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-AVI-010 : Multiples vulnérabilités dans les systèmes SCADA Schneider Electric
– CERTFR-2015-AVI-011 : Vulnérabilité dans Microsoft Windows AppCompat
– CERTFR-2015-AVI-012 : Vulnérabilité dans le service Telnet de Microsoft Windows
– CERTFR-2015-AVI-013 : Vulnérabilité dans le service de profil utilisateur de Microsoft Windows
– CERTFR-2015-AVI-014 : Vulnérabilité dans le composant TS WebProxy de Microsoft Windows
– CERTFR-2015-AVI-015 : Vulnérabilité dans le service NLA de Microsoft Windows
– CERTFR-2015-AVI-016 : Vulnérabilité dans le Rapport d'erreurs de Microsoft Windows
– CERTFR-2015-AVI-017 : Vulnérabilité dans le serveur de stratégie réseau de Microsoft Windows
– CERTFR-2015-AVI-018 : Vulnérabilité dans le pilote WebDAV de Microsoft Windows
– CERTFR-2015-AVI-019 : Multiples vulnérabilités dans Adobe Flash Player
– CERTFR-2015-AVI-020 : Multiples vulnérabilités dans les produits Mozilla
– CERTFR-2015-AVI-021 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
– CERTFR-2015-AVI-022 : Multiples vulnérabilités dans les systèmes SCADA Siemens
– CERTFR-2015-AVI-023 : Multiples vulnérabilités dans les produits Juniper
– CERTFR-2015-AVI-024 : Multiples vulnérabilités dans les produits BlueCoat
– CERTFR-2015-AVI-025 : Vulnérabilité dans IBM AIX
– CERTFR-2015-AVI-026 : Multiples vulnérabilités dans le noyau Linux de Debian
– CERTFR-2015-AVI-027 : Vulnérabilité dans Samba

Gestion détaillée du document

19 janvier 2015 version initiale.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-003