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 janvier 2016
N° CERTFR-2016-ACT-003

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-003

1 - Mise à jour de la note d'information Les bons réflexes en cas d'intrusion sur un système d'information

La note d'information CERTA-2002-INF-002,ayant pour sujet les bons réflexes en cas d'intrusion sur un système d'information a été mise à jour.

La mise à jour concerne la rubrique Les services centraux spécialisés, dans le paragraphe `4.Quels sont les aspects légaux d'une intrusion ?`
Elle peut être consultée au lien suivant :
http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

2 - Mise à jour mensuelle de Microsoft

Le 12 janvier, lors de sa mise à jour mensuelle, Microsoft a publié neuf bulletins de sécurité, dont six considérés critiques et trois importants :

- MS16-001 (critique) concernant Internet Explorer ;
- MS16-002 (critique) concernant Edge ;
- MS16-003 (critique) concernant les moteurs JScript et VBScript ;
- MS16-004 (critique) concernant Microsofts Office ;
- MS16-005 (critique) concernant des pilotes Windows en mode noyau ;
- MS16-006 (critique) concernant Silverlight ;
- MS16-007 (important) concernant Windows ;
- MS16-008 (important) concernant le noyau de Windows ;
- MS16-010 (important) concernant le serveur Exchange.

Navigateurs

Cette mise à jour corrige plusieurs vulnérabilités dans les navigateurs Microsoft de type corruptions de mémoire, au niveau du navigateur lui-même ou du moteur de scripts. Ces vulnérabilités permettent une exécution de code arbitraire à distance avec le niveau de privilèges de l'utilisateur courant. Le CERT-FR en profite pour rappeler ici le principe du moindre privilège, ce qui implique de ne pas naviguer sur Internet à partir d'un compte administrateur.

Une autre vulnérabilité corrigée dans Internet Explorer permet à un attaquant d'élever son niveau de privilèges. De plus, le CERT-FR tient de nouveau à attirer l'attention sur la nouvelle politique de Microsoft concernant le support des navigateurs, entrée en vigueur le 12 janvier 2016 : seule la dernière version d'Internet Explorer sur chaque plate-forme supportée continuera à recevoir des mises à jour de sécurité (voir le bulletin d'actualité CERTFR-2016-ACT-001 pour la liste des combinaisons supportées).

Bureautique

Plusieurs vulnérabilités de type corruption de mémoire ont également été corrigées dans Microsoft Office. Ces vulnérabilités sont susceptibles de permettre une exécution de code à distance lors de l'ouverture d'un fichier spécialement conçu.

Windows

Microsoft corrige également plusieurs vulnérabilités dans Windows permettant soit une exécution arbitraire de code à distance, soit une élévation de privilèges, soit encore un contournement de la politique de sécurité.

Recommandations

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

3 - Rappel des avis émis

Dans la période du 11 au 17 janvier 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-008 : Vulnérabilité dans Cisco Adaptive Security Appliance
- CERTFR-2016-AVI-009 : Vulnérabilité dans Huawei Switch S5300
- CERTFR-2016-AVI-010 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-011 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-012 : Vulnérabilité dans Microsoft JScript et VBScript
- CERTFR-2016-AVI-013 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-014 : Vulnérabilité dans Microsoft Silverlight
- CERTFR-2016-AVI-015 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTFR-2016-AVI-016 : Multiples vulnérabilités dans le noyau de Windows
- CERTFR-2016-AVI-017 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-018 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2016-AVI-019 : Multiples vulnérabilités dans Adobe Acrobat
- CERTFR-2016-AVI-020 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2016-AVI-021 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-022 : Multiples vulnérabilités dans le client d'OpenSSH

Gestion détaillée du document

18 janvier 2016 version initiale.