Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 16 août 2013
N° CERTA-2013-ACT-033

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-033

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-033`

1 Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de *Microsoft*, huit bulletins de sécurité ont été publiés.

Les trois premiers bulletins sont considérés comme critiques :

- MS13-059 qui concerne *Internet Explorer*, cette mise à jour corrige onze vulnérabilités ;
- MS13-060 qui concerne le processeur de scripts Unicode, cette mise à jour corrige une vulnérabilité ;
- MS13-061 qui concerne *Microsoft Exchange Server*, cette mise à jour corrige trois vulnérabilités provenant de *Oracle Outside In*.

Toutes ces vulnérabilités peuvent mener un attaquant à exécuter du code arbitraire à distance.

Cinq bulletins sont considérés comme importants :

- MS13-062 qui concerne le *Remote Procedure Call* (RPC), cette mise à jour corrige une vulnérabilité ;
- MS13-063 qui concerne le noyau *Microsoft Windows*, cette mise à jour corrige quatre vulnérabilités ;
- MS13-064 qui concerne le pilote NAT *Microsoft Windows*, cette mise à jour corrige une vulnérabilités de *Oracle Outside In* ;
- MS13-065 qui concerne *ICMPv6*, cette mise à jour corrige une vulnérabilité ;
- MS13-066 qui concerne *Active Directory Federation Services* (ADFS), cette mise à jour corrige une vulnérabilité.

Le correctif MS13-063 / CVE-2013-2556 est plus amplement détaillé dans ce bulletin d'actualité.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de août 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-aug

2 Correction d'une technique de contournement des protections DEP et ASLR sous Windows

Le 13 août 2013, Microsoft a publié une mise à jour de sécurité qui se distingue des mises à jour habituelles. En effet, celle-ci ne corrige pas une erreur d'implémentation mais supprime un moyen de contourner, sur les systèmes Windows, les techniques de protection ASLR (Address Space Layout Randomization) et le DEP (Data Execution Prevention).

Sous Windows, l'espace mémoire « SharedUserData », qui sert à échanger des informations entre le mode utilisateur et le mode noyau, est toujours accessible à l'adresse 0x7ffe0000. Cet espace contient notamment des pointeurs de fonctions :

- 7ffe0340 77509e69 ntdll!LdrInitializeThunk
- 7ffe0344 774e0124 ntdll!KiUserExceptionDispatcher
- 7ffe0348 774e0028 ntdll!KiUserApcDispatcher
- 7ffe034c 774e00dc ntdll!KiUserCallbackDispatcher
- 7ffe0350 7756fc24 ntdll!LdrHotPatchRoutine
- 7ffe0354 775026d1 ntdll!ExpInterlockedPopEntrySListFault
- 7ffe0358 7750269b ntdll!ExpInterlockedPopEntrySListResume
- 7ffe035c 775026d3 ntdll!ExpInterlockedPopEntrySListEnd
- 7ffe0360 774e01b4 ntdll!RtlUserThreadStart
- 7ffe0364 775735da ntdll!RtlpQueryProcessDebugInformationRemote
- 7ffe0368 77527111 ntdll!EtwpNotificationThread

Parmi ces pointeurs, la fonction « ntdll!LdrHotPatchRoutine » peut être utilisée pour contourner DEP et ASLR. Elle permet en effet de charger de façon arbitraire un fichier DLL local ou pouvant être présent sur un partage réseau.

Le correctif remplace ces adresses de fonctions par des octets nuls, il ne sera donc plus possible d'exploiter de failles via ce contournement. Ce correctif constitue donc une mesure de défense en profondeur contre toute une catégorie de méthodes d'exploitation.

Le CERTA recommande d'appliquer ce correctif le plus rapidement possible sur tous les systèmes Microsoft Windows.

Documentation

- Bulletin de sécurité Microsoft MS13-063 :
  http://technet.microsoft.com/en-us/security/bulletin/MS13-063
- Bulletin de sécurité Microsoft détaillant le correctif :
  http://blogs.technet.com/b/srd/archive/2013/08/12/mitigating-the-ldrhotpatchroutine-dep-aslr-bypass-with-ms13-063.aspx

3 Black Hat USA 2013

La conférence Black Hat s'est déroulée du 27 juillet au 1er août. Elle a regroupé un nombre important de présentations dans divers domaines liés à la cybersécurité. Outre le côté technique de certaines présentations, on peut noter que certains thèmes sont actuellement régulièrement abordés lors de ces évènements.

Parmi ces thèmes d'actualité, on peut noter :

- les menaces envers les systèmes SCADA, industriels et embarqués ;
- les menaces contre les smartphones et les problématiques associées au BYOD (*Bring Your Own Device*) ;
- les attaques menées contre l'UEFI et le *SecureBoot* ;
- les menaces contre les services Web.

Le suivi et l'identification des sujets traités lors de ce genre de conférences permettent une évaluation de la menace et des attaques possibles du moment contre les systèmes d'information.

Documentation

- Conférence Black Hat
  http://www.blackhat.com

4 Rappel des avis émis

Dans la période du 09 au 15 août 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-466 : Multiples vulnérabilités dans Adobe Reader et Acrobat

- CERTA-2013-AVI-467 : Multiples vulnérabilités dans PuTTY
- CERTA-2013-AVI-468 : Multiples vulnérabilités dans Symfony
- CERTA-2013-AVI-469 : Vulnérabilité dans Samba
- CERTA-2013-AVI-470 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-471 : Vulnérabilité dans le processeur de scripts Unicode Microsoft
- CERTA-2013-AVI-472 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTA-2013-AVI-473 : Vulnérabilité dans Microsoft Remote Procedure Call
- CERTA-2013-AVI-474 : Multiples vulnérabilités dans le noyau Microsoft Windows
- CERTA-2013-AVI-475 : Vulnérabilité dans le pilote NAT de Microsoft Windows
- CERTA-2013-AVI-476 : Vulnérabilité dans l'implémentation ICMPv6 de Microsoft Windows
- CERTA-2013-AVI-477 : Vulnérabilité dans Microsoft Active Directory Federation Services

Gestion détaillée du document

16 août 2013 version initiale.