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 01 août 2014
N° CERTFR-2014-ACT-031

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-031

1 - Mitigation des vulnérabilités de type 'use-after-free' dans Microsoft Internet Explorer

Le deuxième mardi de chaque mois, Microsoft publie une série de correctifs de failles de sécurité affectant ses produits. Internet Explorer figure généralement dans la liste, et les corruptions mémoire représentent souvent un fort pourcentage des failles qui y sont corrigées.

Parmi les vulnérabilités liées aux corruptions mémoire, on trouve celle dite « use-after-free » qui correspond à l'utilisation d'un pointeur attardé (« dangling pointer »).

Ce cas résulte de la libération précoce d'une zone mémoire vers laquelle des références subsistent. Si l'une de ces références est employée après libération de la zone mémoire, un comportement erratique pourra en résulter car la zone est susceptible d'avoir été réinscrite. Eventuellement, un attaquant chevronné peut parfois réinscrire la zone mémoire avec un contenu choisi pour provoquer une exécution de code arbitraire.

Or les deux derniers correctifs en date d'Internet Explorer (MS14-035 et MS14-037) introduisent deux contre-mesures intéressantes qui rendent plus difficile l'exploitation des vulnérabilités de type « use-after-free » : il s'agit du Isolated Heap (tas mémoire isolé) et du Protected Free (libération mémoire protégée).

Le principe de fonctionnement du Isolated Heap est d'allouer certaines classes d'objets (notamment la plupart des objets du DOM, ainsi que certains objets décrivant la structure interne d'une page HTML) dans une zone isolée du tas mémoire, de façon à limiter la réutilisation de la mémoire par des objets de classes différentes. En effet, il est courant pour un attaquant de tenter de remplacer un objet libéré par un objet d'un autre type (par exemple une chaîne de caractères JavaScript) dont le contenu est judicieusement choisi pour détourner le flot d'exécution du programme.

Quant au Protected Free, il consiste à retarder dans le temps la réutilisation d'une zone mémoire libérée. En cas de libération intempestive, le bloc mémoire n'est plus immédiatement disponible pour réutilisation, ce qui limite le risque de le voir réallouer aussitôt et ses données remplacées par celles d'un nouvel objet.

Le mécanisme du Protected Free utilise également la présence de références demeurant sur la pile vers un bloc mémoire pour retarder la libération dudit bloc (une technique héritée du glanage de cellule) ce qui devrait drastiquement limiter l'exploitation d'une catégorie de vulnérabilités de type "use-after-free" où les seules références incorrectes à un objet libéré sont situées sur la pile.

Seule l'expérience révèlera l'efficacité de ces contre-mesures. Dans le passé certaines failles sont tombées en désuétude après l'introduction de mécanismes similaires. On ne peut qu'espérer qu'il en sera de même avec cette classe de vulnérabilités.

Il s'agit donc d'une initiative importante de Microsoft dans la mitigation de l'exploitation des vulnérabilitiés "use-after-free", d'autant plus louable qu'elle fait partie des mises à jour automatiques mensuelles de Windows.

En complément de l'application des correctifs mentionnés dans cet article, le CERT-FR recommande de configurer l'outil de prévention EMET (voir le précédent bulletin d'actualité CERTFR-2014-ACT-010).

Documentation

- Bulletin de sécurité Microsoft MS14-035 :
  https://technet.microsoft.com/en-us/library/security/ms14-035.aspx
- Bulletin de sécurité Microsoft MS14-037 :
  https://technet.microsoft.com/en-us/library/security/ms14-037.aspx
- Bulletin d'actualité CERT-FR CERTFR-2014-ACT-010 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-010/CERTFR-2014-ACT-010.html

2 - Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité (PRIS)

Le 28 juillet 2014, l'ANSSI a publié un appel à commentaires pour la publication du référentiel d'exigences applicables aux PRIS.

Ces prestataires auront pour mission de :

- définir une méthode de réponse adaptée au contexte de l'incident de sécurité ;
- collecter et analyser des éléments issus du système d'information ;
- identifier le mode opératoire de l'attaquant ;
- qualifier l'étendue de la compromission ;
- évaluer les risques et les impacts associés ;
- préconiser des mesures de remédiation.

Le référentiel permet de réaliser la qualification des prestataires dans le but de donner aux commanditaires des garanties sur les compétences et sur la qualité des travaux pouvant être réalisés.

Les exigences concernent le prestataire lui-même, les analystes et le déroulement de la prestation.

Les observations, commentaires et propositions peuvent être transmis jusqu'au 31 octobre 2014.

Documentation

- Appel à commentaires sur le référentiel d'exigences applicable aux PRIS :
  http://www.ssi.gouv.fr/fr/menu/actualites/appel-commentaires-referentiel-d-exigences-applicables-pris.html

3 - Rappel des avis émis

Dans la période du 25 au 31 juillet 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-332 : Multiples vulnérabilités dans le noyau Linux de Debian
- CERTFR-2014-AVI-333 : Multiples vulnérabilités dans le noyau Linux de Red Hat Enterprise Linux
- CERTFR-2014-AVI-334 : Multiples vulnérabilités dans le système SCADA SIMATIC WinCC de Siemens
- CERTFR-2014-AVI-335 : Multiples vulnérabilités dans des produits HP et H3C

Gestion détaillée du document

01 août 2014 version initiale.