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 07 novembre 2016
N° CERTFR-2016-ACT-045

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-045

1 - Vulnérabilité de type élévation de privilèges dans Microsoft Windows

Le vendredi 21 octobre 2016, Google a averti Adobe et Microsoft que deux vulnérabilités, jusque là inconnues, étaient activement exploitées dans leurs produits par un groupe d'attaquants persistants et avancés dans le cadre d'attaques ciblées.

La première, une vulnérabilité d'exécution de code à distance, touche Adobe Flash Player et porte l'identifiant CVE-2016-7855. Le 27 octobre, Adobe a publié un correctif la corrigeant[01].

La deuxième touche le noyau de Windows. Elle permet une élévation de privilèges. Aucun correctif n'est pour l'instant disponible, ce qui a déclenché la publication d'une alerte du CERT-FR[02].

Détails de la vulnérabilité

La vulnérabilité est exploitable lors d'un appel à la fonction NtSetWindowLongPtr() prenant en argument un pointeur vers une fenêtre dont les attributs seront spécifiés via l'argument `index`. L'attribut `GWLP_ID` doit être activé ainsi que l'attribut `GWL_STYLE` qui doit être spécifié avec une valeur à `WS-CHILD`[03].

Cette fonction fait partie de la bibliothèque `win32k.sys` présente dans le noyau Windows. Cette bibliothèque est une cible de choix pour les attaquants lorsqu'il s'agit d'élever ses privilèges. Rien que cette année, une trentaine de vulnérabilités d'élévation de privilèges ont été corrigées. Celle dont il est question ici est la troisième à être exploitée activement avant la sortie d'un correctif[04].

Il existe cependant des mesures de contournement pour les utilisateurs de Windows 10. Google Chrome bloque les appels systèmes vers `win32k.sys`[05]. Depuis août dernier et la mise à jour anniversaire, Windows 10 implémente un filtre des appels systèmes vers `win32k.sys` lorsqu'ils proviennent du navigateur *Edge*[06].

Seule la navigation sur internet avec les deux navigateurs susnommés sur un Windows 10 à jour est protégée de cette vulnérabilité. Cependant, même dans ce cas-là, si l'utilisateur télécharge un fichier piégé et l'ouvre, la vulnérabilité pourra être déclenchée.

Utilisée seule, une élévation de privilèges a un impact limité, même si non négligeable. C'est pour cela que l'exploitation de ce type de vulnérabilité est souvent couplée à une exécution de code à distance. En combinant les deux, un attaquant peut alors prendre le contrôle total d'un système.

Dans le cadre de l'attaque détectée par Google, la première vulnérabilité peut désormais être corrigée. Toutefois, la deuxième reste exploitable et peut toujours être réutilisée en l'associant à une autre vulnérabilité d'exécution de code à distance.

Publication

Le 31 octobre 2016, Google a annoncé publiquement l'existence de la vulnérabilité d'élévation de privilèges[07]. Selon leur politique de divulgation publique de vulnérabilités, Google laisse à un développeur quatre-vingt-dix jours pour publier un correctif à partir du moment où celui-ci est notifié. Ce délai est réduit à sept jours en cas d'exploitation active.

Le 1er novembre 2016, Microsoft a reconnu l'existence de cette vulnérabilité[08], tout en indiquant qu'un correctif sera disponible à l'occasion de la prochaine mise à jour mensuelle, c'est à dire le 8 novembre 2016. Dans ce billet, Google est également critiqué pour ne pas avoir attendu la sortie du correctif, car la divulgation augmenterait "le risque encouru par les utilisateurs".

Ce n'est pas la première fois cette année qu'une vulnérabilité Windows est annoncée publiquement lorsque Microsoft n'a pas respecté les délais fixés par Google[09].

Si l'on met de côté les possibles implications financières, il s'agit là d'un cas d'opposition d'annonce responsable ("responsible disclosure") contre annonce totale ("full disclosure"). Dans le cadre d'une annonce responsable, aucune annonce publique n'est faite avant qu'un correctif ne soit disponible. Par opposition, une annonce totale est effectuée à la découverte de la vulnérabilité et ne cache aucun détail. Dans le premier cas, la sécurité repose sur la discrétion cependant il existe un risque d'abus de la part du développeur qui pourrait trop attendre pour fournir un correctif. Dans le deuxième cas, la main de l'éditeur est forcée, l'obligeant à sortir rapidement un correctif, cependant le nombre d'attaquants potentiels va augmenter en attendant que la vulnérabilité soit corrigée.

Ce débat ne date pas d'aujourd'hui[10], et l'objet de ce bulletin n'est pas de l'alimenter.

Recommandations

Le CERT-FR recommande l'application du correctif de sécurité au plus tôt lorsque celui-ci sera disponible. En attendant, les utilisateurs sont invités à la plus grande prudence lors de la navigation sur internet, du téléchargement de fichiers ainsi qu'à l'ouverture de messages électroniques, et ce même si le greffon Flash Player est désactivé dans le navigateur.

Documentation

01 Avis CERT-FR CERTFR-2016-AVI-364
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-364/index.html

02 Alerte CERT-FR CERTFR-2016-ALE-008
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-008/index.html

03 NTSetWindowsLongPtr()
https://msdn.microsoft.com/en-us/library/windows/desktop/ms633591(v=vs.85).aspx

04 MS16-039
https://technet.microsoft.com/fr-fr/library/security/ms16-039.aspx?f=255&MSPPError=-2147217396

05 Verrouillage win32k de Chrome
https://docs.google.com/document/d/1gJDlk-9xkh6_8M_awrczWCaUuyr0Zd2TKjNBCiPO_G4/editheading=h.xgjl2srtytjt

06 Filtre Edge (page 34)
https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf

07 Annonce Google
https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html

08 Annonce Microsoft
https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/

09 Google annonce une vulnérabilité dans Windows début 2016
http://arstechnica.com/security/2015/01/google-sees-a-bug-before-patch-tuesday-but-windows-users-remain-vulnerable/

10 Full Disclosure
https://www.schneier.com/crypto-gram/archives/2001/1115.html

2 - Rappel des avis émis

Dans la période du 31 octobre au 06 novembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-008 : Vulnérabilité dans Microsoft Windows
- CERTFR-2016-AVI-366 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-367 : Vulnérabilité dans Google Chrome
- CERTFR-2016-AVI-368 : Multiples vulnérabilités dans F5 BIG-IP

Gestion détaillée du document

07 novembre 2016 version initiale.

09 novembre 2016 correction horizon de publication Google (quatre-vingt-dix jours au lieu de soixante).

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-2016-ACT-045`