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 27 juillet 2015
N° CERTFR-2015-ACT-030

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-030

1 - Vulnérabilité CVE-2015-2426

Suite à la fuite d'informations subie récemment par la société italienne Hacking Team, l'existence de plusieurs failles non-corrigées a été révélée dans les logiciels Microsoft Windows et Adobe Flash.

En ce qui concerne Windows, la plupart des vulnérabilités ont fait l'objet de correctifs distribués le mardi 14 juillet 2015, lors du cycle mensuel normal de Microsoft.

Cependant la faille CVE-2015-2426, rendue publique le 20 juillet 2015, a nécessité l'émission d'un bulletin exceptionnel MS15-078, en raison de sa criticité et de l'existence avérée d'un code d'exploitation. Elle concerne toutes les versions supportées de Windows, et a donné lieu à l'alerte CERTFR-2015-ALE-008.

Il s'agit d'une faille située dans le composant `ATMFD.DLL` du noyau de Windows (Adobe Type Manager Font Driver, pilote de gestion des polices de caractères au format OpenType). Le bogue dans ce composant permet à un attaquant d'exécuter du code arbitraire en mode noyau, en utilisant un fichier OTF malformé. Il en résulte, d'une part, une élévation de privilèges locale et d'autre part une exécution de code arbitraire à distance rendue possible par le téléchargement automatique des polices de caractères par les navigateurs Web.

Pour ces raisons, Microsoft a qualifié la vulnérabilité de critique et a jugé nécessaire de fournir un correctif hors cycle.

La faille résulte d'un défaut de vérification des paramètres d'une table GPOS (Glyph Positioning Table). Les structures GPOS interviennent normalement dans le crénage des glyphes, c'est-à-dire dans le rendu harmonieux des signes typographiques.

Le paramètre en question, lorsqu'il vaut zéro, provoque l'allocation d'un bloc de taille nulle sur le tas du noyau. Par la suite, des données sont copiées dans le bloc, provoquant un débordement sur le bloc suivant. En manipulant l'organisation du tas, un attaquant peut corrompre des structures critiques du noyau et en prendre le contrôle.

Le correctif introduit par Microsoft dans la dernière version du code consiste à vérifier que le paramètre fautif ne puisse pas être nul.

Le CERT-FR recommande d'appliquer le correctif de Microsoft au plus vite. Pour les utilisateurs avancés de Windows, Microsoft décrit également dans le bulletin MS15-078 des méthodes de désactivation du composant `ATMFD.DLL`, soit par renommage du fichier en question, soit par une modification dans la base de registre pour les systèmes Windows 8.

Pour les utilisateurs n'ayant aucun besoin de rendu des fontes OpenType, il est ainsi possible de se préserver d'éventuelles futures failles dans le même composant. En effet, ce n'est pas la première fois que la bibliothèque `ATMFD.DLL` est prise pour cible, et l'historique des failles qui lui sont attribuées suggère que ce ne sera pas la dernière.

Documentation

- Bulletin MS15-078 de Microsoft:
  https://technet.microsoft.com/en-us/library/security/ms15-078.aspx

– Alerte du CERT-FR:
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-008/index.html

2 - Rappel des avis émis

Dans la période du 20 au 25 juillet 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-ALE-008 : Vulnérabilité dans le pilote de gestion des polices de caractères de Microsoft Windows
– CERTFR-2015-ALE-009 : Vulnérabilité dans Apple Mac OS X
– CERTFR-2015-AVI-312 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2015-AVI-313 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2015-AVI-314 : Multiples vulnérabilités dans les produits SCADA Siemens
– CERTFR-2015-AVI-315 : Multiples vulnérabilités dans les produits SCADA Schneider
– CERTFR-2015-AVI-316 : Vulnérabilité dans WordPress
– CERTFR-2015-AVI-317 : Multiples vulnérabilités dans les produits BlueCoat
– CERTFR-2015-AVI-318 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

27 juillet 2015 version initiale.