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 20 mars 2017
N° CERTFR-2017-ACT-012

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-012

1 - Mise à jour mensuelle de Microsoft

Le 14 mars 2017, lors de sa mise à jour mensuelle, Microsoft a publié dix-huit bulletins de sécurité, dont neuf sont considérés comme critiques et huit comme importants :

- MS17-006 (critique) concernant Internet Explorer ;
- MS17-007 (critique) concernant Microsoft Edge ;
- MS17-008 (critique) concernant Windows Hyper-V ;
- MS17-009 (critique) concernant la bibliothèque PDF Microsoft Windows ;
- MS17-010 (critique) concernant le serveur SMB Microsoft Windows ;
- MS17-011 (critique) concernant Microsoft Uniscribe ;
- MS17-012 (critique) concernant Microsoft Windows ;
- MS17-013 (critique) concernant Microsoft Graphics ;
- MS17-023 (critique) concernant Adobe Flash Player ;
- MS17-014 (important) concernant Microsoft Office ;
- MS17-015 (important) concernant Microsoft Exchange Server ;
- MS17-016 (important) concernant Windows IIS ;
- MS17-017 (important) concernant le noyau Windows ;
- MS17-018 (important) concernant les pilotes en mode noyau Windows ;
- MS17-019 (important) concernant Active Directory Federation Services ;
- MS17-020 (important) concernant Création de DVD Windows ;
- MS17-021 (important) concernant Windows DirectShow ;
- MS17-022 (important) concernant Microsoft XML Core Services.

Navigateurs

Cette mise à jour corrige douze vulnérabilités dans Internet Explorer. Cinq permettent une exécution de code à distance et sont considérées comme critiques. Elles sont déclenchées par des corruptions de mémoire.

Quatre autres vulnérabilités débouchent sur des fuites d'informations et sont jugées comme importantes. Deux autres peuvent conduire à une usurpation d'identité. Enfin, une vulnérabilité permet une élévation de privilèges.

Parmi les vulnérabilités corrigées dans Internet Explorer, cinq étaient connues publiquement. Parmi celles-ci, la CVE-2017-0037 avait été dévoilée au mois de février. Elle permet à un attaquant d'exécuter du code arbitraire à distance. Cette vulnérabilité a fait l'objet d'un bulletin d'alerte du CERT-FR.

De plus, d'après le bulletin de sécurité de Microsoft, la vulnérabilité CVE-2017-0149 est exploitée activement.

Concernant Microsoft Edge, trente-deux vulnérabilités ont été corrigées : vingt-et-une conduisent à des exécutions de code arbitraire à distance (vingt sont critiques et la dernière est indiquée comme étant importante). Parmi ces vingt-et-une vulnérabilités, dix-huit sont liées à une altération de la mémoire dans le moteur de script.

Cinq vulnérabilités importantes peuvent mener à la divulgation d'informations. Enfin, trois vulnérabilités permettant une usurpation d'identité et trois vulnérabilités permettant de contourner la fonctionnalité de sécurité sont jugées importantes.

Sur l'ensemble des vulnérabilités corrigées par ce bulletin, cinq étaient connues publiquement. Quatre vulnérabilités sont partagées avec Internet Explorer, notamment CVE-2017-0037, CVE-2017-0012 et CVE-2017-0033.

Adobe a corrigé sept vulnérabilités pour le module Flash Player intégré dans Internet Explorer et Edge. Jugées comme critiques, six d'entres elles peuvent conduire à une exécution de code et la dernière concerne une divulgation d'information.

Bureautique

Douze vulnérabilités sont corrigées pour Microsoft Office : sept d'entre elles peuvent conduire à une exécution de code arbitraire à distance et sont jugées comme importantes. Ces vulnérabilités sont liées à une altération de la mémoire de Microsoft Office. Deux corrections portent sur des vulnérabilités conduisant à des divulgations d'informations. Ces vulnérabilités, répertoriées sous les références CVE-2017-0027 et CVE-2017-0105, sont décrites comme importantes.

Une vulnérabilité classée comme importante peut provoquer un déni de service. Cette vulnérabilité, la CVE-2017-0029, peut être déclenchée avec un fichier malveillant conçu spécialement. Il est à noter que cette vulnérabilité était connue publiquement.

Une vulnérabilité importante affectant Microsoft Lync pour Mac tire parti d'une erreur de validation de certificats afin de provoquer un contournement de la fonctionnalité de sécurité.

Enfin, une vulnérabilité de type script de site à site (XSS), la CVE-2017-0107, peut permettre une élévation de privilèges en autorisant l'exécution de script dans le contexte de l'utilisateur visé. Cette faille est considérée comme importante par Microsoft.

Windows

Parmi les bulletins traitant de vulnérabilité affectant les systèmes Windows, six sont considérés comme critiques et huit avec une sévérité importante.

Le composant Microsoft Graphics voit la correction de douze vulnérabilités. Au sein de ces correctifs, deux adressent des vulnérabilités permettant une exécution de code à distance et sont jugées critiques. L'une d'elles, la CVE-2017-0014, était connue publiquement avant la publication du bulletin de Microsoft. Pour ce composant, on notera de plus la correction de la vulnérabilité CVE-2017-0005. Cette vulnérabilité importante permet une élévation de privilèges et est reportée comme étant exploitée dans la nature.

Vingt-neuf correctifs sont apportés pour Microsoft Uniscribe. Huit, critiques, corrigent des vulnérabilités liées à de l'exécution de code à distance. Les vingt-et-un autres sont des correctifs se rapportant à des divulgations d'informations. Ces derniers sont considérés comme importants.

Plusieurs correctifs sont disponibles pour Windows Hyper-V. Quatre sont rattachés à des vulnérabilités d'exécution de code à distance jugées critiques. Pour les autres correctifs, six seront destinés à des vulnérabilités de déni de service. Un dernier correctif sera aussi publié pour une vulnérabilité donnant lieu à une divulgation d'information.

Le bulletin MS17-012 corrige six vulnérabilités dans Windows. Parmi ces vulnérabilités, la CVE-2017-0104, une altération de mémoire dans ISNS Server permet de provoquer une exécution de code à distance et est jugée critique. On notera aussi la présence d'un correctif pour la CVE-2017-0016, révélée publiquement avant la publication de ce bulletin et pouvant causer un déni de service *via* un déréférencement NULL dans SMBv2/SMBv3.

Le serveur SMB Microsoft Windows bénéficie par ailleurs de six correctifs pour six vulnérabilités critiques. Cinq correspondent à une exécution de code à distance, la dernière vulnérabilité étant une divulgation d'informations.

Enfin, une mise à jour de sécurité est disponible pour la CVE-2017-0023. Cette vulnérabilité critique relative à la bibliothèque PDF Microsoft Windows tire parti d'une altération de la mémoire afin d'exécuter du code arbitraire à distance.

Au travers des huit bulletins consacrés à des mises à jour de sécurité importantes, Microsoft corrige dix-huit vulnérabilités. Quatre correctifs visent des vulnérabilités de divulgation d'informations. Un correctif pour une divulgation d'information dans Microsoft XML Core Services est notamment déployé pour la CVE-2017-0022, noté comme étant déjà exploitée. Les dix autres corrections apportées par ces mises à jour sont relatives à des

vulnérabilités d'élévation de privilèges. On notera parmi celles-ci la CVE-2017-0050 permettant une élévation de privilèges dans le noyau Windows, déjà connue publiquement.

Recommandations

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

En outre, on notera que le bulletin MS17-010 corrige plusieurs vulnérabilités impactant le service SMB permettant la prise de contrôle d'un système vulnérable à distance sans authentification au préalable. Le CERT-FR rappelle que Microsoft ne publie plus de correctifs de sécurité pour les systèmes antérieurs à Windows Vista. Ainsi les systèmes Windows XP et Windows Server 2003 ne disposeront pas de correctifs pour cette vulnérabilité critique.

Le CERT-FR rappelle donc l'importance de maintenir son système à jour, et de déployer un système supporté par l'éditeur pouvant bénéficier des correctifs de sécurité apportés par ce dernier.

Documentation

- https://technet.microsoft.com/fr-fr/library/security/MS17-006
- https://technet.microsoft.com/fr-fr/library/security/MS17-007
- https://technet.microsoft.com/fr-fr/library/security/MS17-008
- https://technet.microsoft.com/fr-fr/library/security/MS17-009
- https://technet.microsoft.com/fr-fr/library/security/MS17-010
- https://technet.microsoft.com/fr-fr/library/security/MS17-011
- https://technet.microsoft.com/fr-fr/library/security/MS17-012
- https://technet.microsoft.com/fr-fr/library/security/MS17-013
- https://technet.microsoft.com/fr-fr/library/security/MS17-014
- https://technet.microsoft.com/fr-fr/library/security/MS17-015
- https://technet.microsoft.com/fr-fr/library/security/MS17-016
- https://technet.microsoft.com/fr-fr/library/security/MS17-017
- https://technet.microsoft.com/fr-fr/library/security/MS17-018
- https://technet.microsoft.com/fr-fr/library/security/MS17-019
- https://technet.microsoft.com/fr-fr/library/security/MS17-020
- https://technet.microsoft.com/fr-fr/library/security/MS17-021
- https://technet.microsoft.com/fr-fr/library/security/MS17-022
- https://technet.microsoft.com/fr-fr/library/security/MS17-023
- http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-002/
- http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-003/

2 - Publication récente d'une vulnérabilité critique dans Apache Struts 2

Apache Struts est un cadriciel (*framework*) disponible en source ouverte et qui permet de développer des applications Web avec le langage Java (J2EE).

Le 6 mars 2017, la fondation Apache a publié une alerte de sécurité de niveau élevé concernant une vulnérabilité découverte dans le projet Apache Struts 2 (cf. Documentation - [1]). La vulnérabilité découverte, identifiée comme CVE-2017-5638, peut en effet conduire à des attaques de type "RCE" (*Remote Code Execution*), c'est-à-dire d'exécution de code à distance sur le serveur Web affecté (cf. Documentation - [2]). De plus, cette vulnérabilité est actuellement activement exploitée puisque des preuves de faisabilité sont publiquement disponibles sur Internet depuis cette annonce, afin de démontrer la facilité de mise en oeuvre des attaques.

Suite à la publication de cette vulnérabilité et d'un correctif de sécurité par Apache, le CERT-FR a émis l'alerte "CERTFR-2017-ALE-004" (cf. Documentation - [3]) compte tenu du niveau de risque pour les serveurs vulnérables et de l'exploitation massive par les attaquants. Le CERT-FR a constaté une recrudescence des intrusions informatique à l'aide de cette vulnérabilité.

Vulnérabilité CVE-2017-5638

Description de la vulnérabilité

La vulnérabilité CVE-2017-5638 est introduite par un mauvais traitement de l'analyseur (*parser*) Multipart "Jakarta", lors d'un transfert de fichier depuis un client vers le serveur Web sur lequel est utilisé Apache Struts 2.

Cet analyseur est chargé de vérifier l'en-tête `Content-Type` de la requête HTTP émise par le client, et de traiter les données reçues.

L'exploitation de cette vulnérabilité par un attaquant est donc possible en envoyant une requête HTTP spécialement forgée au serveur vulnérable. Il suffit en effet que le champ d'en-tête `Content-Type` de cette requête comporte la valeur `multipart/form-data`, accompagnée d'une expression OGNL (*Object Graph Navigation Language*).

Dans ce cas, Jakarta va évaluer le fragment de code OGNL reçu (cf. Documentation - [4]) : si ce dernier contient des commandes (passées via une chaîne `cmd=`), elles seront alors exécutées avec les droits de l'utilisateur associé au service Web, permettant ainsi un contrôle à distance du serveur par l'attaquant.

Tests de vulnérabilité

Exemple de tentative d'exploitation observée par le CERT-FR :

```
Content-Type:%{(#nike='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):((#container=
#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='echo "Struts2045"').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).
(#p=newjava.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).(#process=#p.start()).
(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

Il s'agit ici simplement d'un test de vulnérabilité : si la page renvoyée par le serveur contient la chaîne "Struts2045", alors celui-ci est vulnérable.

Un autre test de vulnérabilité est proposé par Qualys (cf. Documentation - [5]). Il consiste à envoyer un `Content-Type` qui comporte un code visant à demander, dans la réponse du serveur testé, un nouveau champ d'en-tête ("X-Qualys-Struts") : si celui-ci est effectivement présent et contient "16256160", soit le résultat du calcul 3195*5088, alors le serveur est vulnérable.

```
Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHe
```

Versions d'Apache Struts 2 vulnérables

La vulnérabilité affecte les versions de Struts suivantes :

- de Struts 2.3.5 à Struts 2.3.31
- de Struts 2.5 à Struts 2.5.10

Recommandations

Au vu de l'impact et du faible niveau de technicité nécessaire à l'exploitation de cette vulnérabilité, le CERT-FR recommande le déploiement du correctif dans les plus brefs délais, en appliquant la mise à jour Struts 2.3.32 ou Struts 2.5.10.1. Si les applications vulnérables contiennent des données sensibles, il est également fortement conseillé de les désactiver tant que la mise à jour n'a pas été appliquée. Dans son bulletin de sécurité, Apache propose également de remplacer Jakarta par une implémentation différente de l'analyseur Multipart (cf. Documentation - [1]).

Si le correctif de sécurité ne peut être déployé rapidement, des solutions de contournement temporaires sont proposées par Apache (cf. Documentation - [1]) pour limiter l'exposition d'un serveur vulnérable, à court terme.

La première repose sur l'implémentation d'un filtre *Servlet* qui vérifie le `Content-Type` et rejette les requêtes comportant une valeur différente de `multipart/form-data`. La seconde solution consiste à retirer l'intercepteur de chargement de fichier dans la pile d'intercepteurs.

Il est également envisageable de mettre en place une règle de WAF (*Web Application Firewall*) pour filtrer les requêtes comportant une valeur de `Content-Type` différente de `multipart/form-data` (cf. Documentation - [5] et [6]).

Documentation

1 Bulletin de sécurité Apache (S2-045) :
https://cwiki.apache.org/confluence/display/WW/S2-045

2 Référence CVE (CVE-2017-5638) :
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

3 Bulletin d'alerte du CERT-FR (CERTFR-2017-ALE-004) :
http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-004/index.html

4 Billet Trend Micro :
http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/

5 Billet Qualys :
https://blog.qualys.com/securitylabs/2017/03/14/apache-struts-cve-2017-5638-vulnerability-and-the-qualys-solution

6 Billet Akamai :
https://blogs.akamai.com/2017/03/vulnerability-found-in-apache-struts.html

3 - Rappel des avis émis

Dans la période du 13 au 19 mars 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-075 : Vulnérabilité dans SCADA Wonderware by Schneider Electric Tableau Server
- CERTFR-2017-AVI-076 : Vulnérabilité dans VMware Workstation et Fusion
- CERTFR-2017-AVI-077 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2017-AVI-078 : Vulnérabilité dans Adobe Shockwave Player
- CERTFR-2017-AVI-079 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2017-AVI-080 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2017-AVI-081 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2017-AVI-082 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2017-AVI-083 : Vulnérabilité dans Xen
- CERTFR-2017-AVI-084 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-085 : Multiples vulnérabilités dans Drupal
- CERTFR-2017-AVI-086 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2005-INF-003-016 : Les systèmes et logiciels obsolètes (Actualisation et mise à jour des versions de tous les systèmes et de logiciels.)

Gestion détaillée du document

20 mars 2017 version initiale.