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 18 avril 2017
N° CERTFR-2017-ACT-016

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-016

1 - Fuite de codes d'attaques attribués au groupe Equation

Le vendredi 14 avril 2017, des attaquants se faisant appeler les Shadow Brokers ont publiquement révélé des outils offensifs et des documents, qu'ils affirment provenir d'Equation, un groupe d'élite lié à la NSA.

Parmi ces outils se trouvent entre autres des codes malveillants dont la fonction est d'exploiter des vulnérabilités dans les produits Microsoft.

Microsoft au travers d'un billet le 14 avril 2017 informe ses clients que les exploits suivants ont fait l'objet d'un correctif de sécurité (cf. section Documentation):

- `ETERNALCHAMPION`: affectant SMBV1, CVE 2017-0146 & CVE-2017-0147 ;
- `ETERNALSYNERGY`: affectant SMBv3, MS17-010 ;
- `ETERNALBLUE`: affectant SMBv2, MS17-010 ;
- `ETERNALROMANCE`: affectant SMBv1, MS17-010 ;
- `ESKIMOROLL`: affectant Kerberos, MS14-068 ;
- `EMERALDTHREAD`: affectant SMB, MS10-061 ;
- `EDUCATEDSCHOLAR`: affectant SMB, MS09-050 ;
- `ECLIPSEDWING`: affectant server service, MS08-067 ;
- `ERRATICGOPHER`: affectant SMBv1, corrigé avant la sortie de Windows Vista.

Microsoft a informé ses clients que les codes d'exploitation ENGLISHMANDENTIST, ESTEEMAUDIT et EXPLODINGCAN n'avaient pu être déclenchés sur ses produits encore maintenus: Windows 7 et versions plus récentes, ainsi que Exchange 2010 et versions plus récentes. Le CERT-FR déconseille fortement l'utilisation de produits qui ne sont plus maintenus ou qui sont en fin de vie et invite à mettre à jour les produits qui sont encore maintenus afin de minimiser les risques d'exploitation d'une vulnérabilité.

Documentation

- Billet Microsoft Technet
  https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/

2 - Mise à jour mensuelle de Microsoft

Le 11 avril 2017, Microsoft a publié ses mises à jour mensuelles de sécurité. Cinquante-trois vulnérabilités ont été corrigées, parmi lesquelles vingt sont considérées critiques, trente et une comme importantes et deux comme modérées. Les produits suivants sont affectés :

- Internet Explorer ;
- Microsoft Edge ;

– Microsoft Windows ;
– Microsoft Office et Microsoft Office Services et Web Apps ;
– Visual Studio pour Mac ;
– Le cadriciel .Net ;
– Silverlight ;
– Adobe Flash Player.

Navigateurs

Cette mise à jour corrige trois vulnérabilités dans Internet Explorer. Deux d'entre elles, les vulnérabilités CVE-2017-0201 et CVE-2017-0202, permettent une exécution de code à distance et sont considérées comme critiques. Elles sont déclenchées par des corruptions de mémoire. La troisième permet une élévation de privilèges. Microsoft indique que cette vulnérabilité, notée CVE-201-0210, est activement exploitée dans le cadre d'attaques ciblées.

Edge a reçu cinq correctifs. Trois concernent des vulnérabilités d'altération de mémoire permettant une exécution de code arbitraire à distance. La vulnérabilité CVE-2017-0208 permet une divulgation d'information. La dernière vulnérabilité est jugée modérée et permet un contournement de la fonctionnalité de sécurité.

Adobe a corrigé sept vulnérabilités pour le module Flash Player intégré dans Internet Explorer et Edge. Jugées comme critiques, elles peuvent conduire à une exécution de code arbitraire à distance.

Bureautique

Sept vulnérabilités sont corrigées pour Microsoft Office : trois d'entre elles peuvent conduire à une exécution de code arbitraire à distance, dont deux sont jugées comme critiques.

En particulier, la vulnérabilité CVE-2017-0199 a été exploitée en masse pour distribuer le maliciel `Dridex`. Celle-ci a fait l'objet d'une alerte du CERT-FR (cf. section Documentation). Pour rappel, la vulnérabilité exploitée est déclenchée lors de l'ouverture d'un document Microsoft Word contenant un objet `StdOleLink`. Le processus `winword.exe` effectue alors une requête HTTP vers un serveur de l'attaquant pour télécharger un fichier au format HTA contenant un script malveillant qui sera ensuite exécuté. Si la fonctionnalité `Protected View` est activée, ce qui est le cas par défaut pour les versions 2013 et 2016 d'Office, la vulnérabilité ne peut pas être déclenchée. Cependant, la vulnérabilité CVE-2017-0204, fraîchement corrigée, permet de contourner ce mécanisme de protection. A noter qu'ouvrir un document piégé exploitant la vulnérabilité CVE-2017-0199 avec un autre logiciel de traitement de texte sur Windows ne constitue pas une mesure de contournement effective car le code malveillant peut être également exécuté. Le CERT-FR a pu, par exemple, confirmer que c'est le cas avec LibreOffice.

Les trois autres vulnérabilités affectant la suite Office, référencées CVE-2017-0194, 2017-0195 et 2017-0207, permettent respectivement, une divulgation d'informations, une élévation de privilèges et une usurpation d'identité.

Windows

Vingt-neuf vulnérabilités ont été corrigées dans les divers composants de Windows. Cinq d'entre elles sont critiques et permettent une exécution de code arbitraire à distance. Les vingt-quatre autres sont jugées importantes et sont réparties en cinq catégories : une exécution de code arbitraire à distance, six divulgations d'informations, six élévations de privilèges, un contournement de la fonctionnalité de sécurité et dix dénis de services.

La vulnérabilité CVE-2013-6629 concerne Silverlight et permet une divulgation d'information.

Enfin, la vulnérabilité critique CVE-2017-0160 est corrigée dans le cadriciel .NET et rend possible une exécution de code arbitraire à distance.

Recommandations

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

Documentation

– Bulletin de sécurité Microsoft du 11 avril 2017
https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/42b8fa28-9d09-e711-80d9-000d3a32fc99

– Alerte CERT-FR CERTFR-2017-ALE-007
http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-007/

3 - Rappel des avis émis

Dans la période du 10 au 18 avril 2017, le CERT-FR a émis les publications suivantes :

– CERTFR-2017-AVI-105 : Multiples vulnérabilités dans Adobe Flash Player
– CERTFR-2017-AVI-106 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTFR-2017-AVI-107 : Multiples vulnérabilités dans Microsoft Edge
– CERTFR-2017-AVI-108 : Multiples vulnérabilités dans Microsoft Office
– CERTFR-2017-AVI-109 : Multiples vulnérabilités dans Microsoft Windows
– CERTFR-2017-AVI-110 : Multiples vulnérabilités dans les produits Microsoft
– CERTFR-2017-AVI-111 : Multiples vulnérabilités dans les produits Juniper
– CERTFR-2017-AVI-112 : Multiples vulnérabilités dans ISC BIND
– CERTFR-2017-AVI-113 : Vulnérabilité dans Citrix NetScaler Gateway
– CERTFR-2017-AVI-114 : Multiples vulnérabilités dans Wireshark
– CERTFR-2017-AVI-115 : Vulnérabilité dans VMware vCenter Server
– CERTFR-2017-AVI-116 : Multiples vulnérabilités dans Apache Tomcat
– CERTFR-2017-ALE-008 : Vulnérabilité dans RDP pour Microsoft Windows XP et Windows Server 2003

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2017-ALE-007 : Vulnérabilité dans Microsoft Office (clôture de l'alerte.)

Gestion détaillée du document

18 avril 2017 version initiale.