

**Microsoft Services**

**Table Ronde Sécurité**

**Compte-Rendu**

**du 19 Août 2015**

### Sommaire

Introduction 2

Bulletins de sécurité 2

MS15-093 2

Ressources 3

L’OBJET DU PRESENT DOCUMENT EST DE VOUS FOURNIR L’INFORMATION QUE VOUS AVEZ DEMANDEE CONCERNANT LA SECURITE. GENERALEMENT, L’INFORMATION PROVOQUE UNE PRISE DE CONSCIENCE AUTOUR DE LA SECURITE ET IDENTIFIE LE PERSONNEL, LES PROCEDES, RESSOURCES  ET TECHNOLOGIES QUI SONT  DESTINES A PROMOUVOIR DE BONNES REGLES DE SECURITE DANS VOTRE ORGANISATION.  LES VIRUS ET AUTRES TECHNOLOGIES NUISIBLES DESTINES A ATTAQUER VOTRE ENVIRONNEMENT INFORMATIQUE CHANGENT CONTINUELLEMENT AFIN DE CONTOURNER LES MESURES DE SECURITE EXISTANTES. DES LORS, MAINTENIR UN ENVIRONNEMENT INFORMATIQUE FIABLE EST UN PROCESSUS CONTINU QUI EXIGE QUE VOUS MAINTENIEZ UN PERSONNEL, DES PROCEDES, RESSOURCES ET TECHNOLOGIES ADEQUATS AFIN DE VOUS PROTEGER CONTRE TOUTE ATTEINTE À LA  SECURITE. AUCUNE DISPOSITION CONTENUE DANS LES PRESENTES NE DOIT ETRE INTERPRETEE OU CONSIDEREE COMME UNE CERTIFICATION, UNE GARANTIE  OU TOUTE AUTRE FORME DE VALIDATION QUE VOTRE ENVIRONNEMENT INFORMATIQUE EST ET DEMEURERA PROTEGE CONTRE DES ATTEINTES À LA SECURITE ET NOUS N’ASSUMONS AUCUNE RESPONSABILITE POUR TOUTE ATTEINTE À LA SECURITE OU TOUT DOMMAGE OU PERTE SUBSEQUENT.

TOUTES COMMUNICATIONS OU TRANSMISSIONS D’INFORMATION QUI VOUS SONT ADRESSEES AU SUJET DE MICROSOFT ET CONCERNANT LA SECURITE INCLUANT NOTAMMENT TOUTES SUGGESTIONS, ANALYSES, OU COMMENTAIRES QUI VOUS SONT FOURNIS DURANT UNE ANALYSE RELATIVE À LA SECURITE OU TOUTE AUTRE INFORMATION PASSEE, PRESENTE OU FUTURE RELATIVE NOTAMMENT AUX TESTS DE SECURITE, EVALUATIONS, DISPONIBILITES, HORAIRES OU OBJECTIFS (CI-APRES COLLECTIVEMENT DENOMMES « INFORMATIONS SUR LA SECURITE »), SONT FOURNIS CONFORMEMENT AUX CONDITIONS DU CONTRAT DE SERVICE EXISTANT ENTRE VOUS ET MICROSOFT ET UNIQUEMENT AFIN DE VOUS PERMETTRE DE VOUS ORGANISER FACE A D’EVENTUELS PROBLEMES DE SECURITE. TOUTES LES INFORMATIONS SUR LA SECURITE CONTIENNENT TOUTES LES DONNEES QUI NOUS SONT ACTUELLEMENT ACCESSIBLES MAIS QUI SONT SUSCEPTIBLES DE CHANGER EN RAISON DU CHANGEMENT CONSTANT DE CES DONNEES SANS QUE MICROSOFT VOUS AIT PREALABLEMENT INFORME DE CES CHANGEMENTS. NOUS VOUS RECOMMANDONS DONC DE VERIFIER REGULIEREMENT AUPRES DE NOUS ET SUR LE SITE INTERNET DE SECURITE SITUE À L’ADRESSE SUIVANTE [WWW.MICROSOFT.COM/SECURITY](http://WWW.MICROSOFT.COM/SECURITY) SI LES INFORMATIONS QUE NOUS VOUS AVONS FOURNIES FONT L’OBJET DE MISES À JOUR. VEUILLEZ NOUS CONTACTER SI VOUS AVEZ D’AUTRES QUESTIONS CONCERNANT DES PROBLEMES DE SECURITE OU SI VOUS AVEZ BESOIN D’UNE MISE A JOUR DES INFORMATIONS QUE NOUS VOUS AVONS FOURNIES.

# Introduction

La dernière Table Ronde sécurité consacrée au bulletin de sécurité hors cycle MS15-078 a eu lieu **le mardi 21 juillet 2015** avec une session de questions-réponses dont vous trouverez ci-dessous le compte rendu.

# Bulletins de sécurité

## MS15-093

Q : L'exploitation est-elle liée à une version particulière d'Internet Explorer ou est-elle multi version ?

R : Toutes les versions d'Internet Explorer sont impactées à l'exception de Microsoft Edge. Une exploitation a été constatée, cependant aucun détail n’est disponible. Un POC (Proof of Concept) circule sur Internet.

Q : Quel est l’ordre d’application des mises à jour ?

R : Sur Windows 10, la mise à jour est cumulative. En revanche, sur les versions antérieures, il faut d’abord installer le patch d’août avant d’appliquer celui-ci.

Q : Si le patch du mois d’août ainsi que celui du bulletin hors cycle ne sont pas installés, est-ce que WSUS est capable de déployer les patchs dans le bon ordre ?

R : L’ordonnancement se fait de manière automatique.

Q : Est-ce qu’un redémarrage est nécessaire entre l’application de la mise à jour cumulative d’août et l’installation de ce correctif de sécurité ?

R : Oui, un redémarrage est nécessaire entre les deux installations.

Q : Le risque est-il diminué si nous n’utilisons pas de navigateurs depuis les serveurs de production ?

R : Oui, le risque est diminué sur les serveurs. La sévérité du bulletin est "modérée" uniquement pour toutes les versions "serveur".

Q : Quelle configuration d'EMET permet de contribuer à l'atténuation de cette attaque ?

R : La configuration d’EMET permettant de contribuer à l'atténuation de cette attaque est l’utilisation des paramètres par défaut qui se trouvent dans le fichier « **Recommended Software.xml** »

Q : Quels sont les numéros de KB du 11 août à installer au préalable ?

R : Il faut dans un premier temps installer le KB3078071 puis le KB3087985.

Q : Y-a-t-il des effets de bord à installer ce patch notamment si la mise à jour cumulative d'août ne l'a pas été?

R : Oui, car le patch a été élaboré sur des composants qui n’ont pas le même niveau de compatibilité que ceux utilisés sur la mise à jour d’août. Voir la FAQ du bulletin de sécurité pour plus de détails.

Q : Y-a-t-il un impact potentiel de dysfonctionnement de nos applications après installation des KB?

R : A l’heure actuelle, il n’y a pas de remontée de dysfonctionnement. Par ailleurs, ce patch permet de fixer l'allocation de mémoire.

Q : En juin, la KB3058515 ne permettait plus l'installation de contrôles activeX, une correction a été faite (3072449). Ce hotfix présente t il un risque analogue ?

R : Non, il ne touche pas aux contrôles Active X

Q : Est-ce que le CU d'Août à lui-même des dépendances à installer au préalable ?

Oui, il existe des dépendances pour Office et NotePad (MS 15-081 et MS 15-088) à installer au préalable

## Ressources

* Synthèse des Bulletins de sécurité
[*http://technet.microsoft.com/fr-fr/security/bulletin/MS15-aug*](http://technet.microsoft.com/fr-fr/security/bulletin/MS15-aug)
* Bulletins de sécurité
[*http://technet.microsoft.com/fr-fr/security/bulletin*](http://technet.microsoft.com/fr-fr/security/bulletin)
* Échelle des indices de gravité des bulletins de sécurité du MSRC <http://www.microsoft.com/france/technet/security/bulletin/rating.mspx>
* Webcast des Bulletins de sécurité
[*http://technet.microsoft.com/fr-fr/security/bulletin*](http://technet.microsoft.com/fr-fr/security/bulletin)
* Avis de sécurité
[*http://technet.microsoft.com/fr-fr/security/advisoryarchive/Microsoft-Security-Advisory-Archive*](http://technet.microsoft.com/fr-fr/security/advisoryarchive/Microsoft-Security-Advisory-Archive)
* Abonnez-vous à la synthèse des Bulletins de sécurité (en français)
[*http://www.microsoft.com/france/securite/newsletters.mspx*](http://www.microsoft.com/france/securite/newsletters.mspx)
* Blog du MSRC (Microsoft Security Response Center)
[*http://blogs.technet.com/msrc*](http://blogs.technet.com/msrc)
* Microsoft France sécurité
[*http://www.microsoft.com/france/securite*](http://www.microsoft.com/france/securite)
* TechNet sécurité
[*http://www.microsoft.com/france/technet/security*](http://www.microsoft.com/france/technet/security)