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 février 2017
N° CERTFR-2017-ACT-008

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-008

1 - Report de la mise à jour mensuelle de Microsoft

La mise à jour mensuelle de Microsoft, initialement planifiée pour le mardi 14 février 2017, ne sera pas réalisée ce mois. Les correctifs de l'éditeur devraient être inclus dans la version du mois de mars. Microsoft informe que ce report fait suite à la découverte d'un problème pouvant impacter ses clients.

Documentation

https://blogs.technet.microsoft.com/msrf/2017/02/14/february-2017-security-update-release/

2 - Sensibilisation aux dangers du "remplissage automatique"

En 2010, Google a ajouté dans son navigateur la fonctionnalité de remplissage automatique de champs d'un formulaire. Le principe, bien connu de tous, est de pré-remplir certains champs d'un formulaire (lors de la création d'un compte sur un site par exemple). Cependant, il s'avère qu'un attaquant peut exploiter cette fonctionnalité pour obtenir certaines informations personnelles stockées par le navigateur web. Cette fonctionnalité permet de stocker dans le navigateur des champs tels que le nom, la ville, le code postal, le pays, etc., mais également des informations bancaires comme le numéro de carte, la date d'expiration, ou bien le possesseur de la carte. Pour exploiter cette fonctionnalité, l'attaquant va mettre en place un formulaire sur un site web et ajouter des champs cachés correspondant aux données qui l'intéressent. Une première approche serait d'utiliser un tag "hidden" pour le type de du champs :

```
<input type=hidden name=item_no value=00001>
```

Cependant, dans plusieurs navigateurs, les champs de type hidden ne sont pas préremplis par le navigateur et donc cela ne fonctionne pas. Une seconde approche est de cacher les champs voulus à la suite d'un champ légitime, en utilisant l'attribut "overflow:hidden" du style de la balise "div" :

```
<table><tr><td><div style="overflow:hidden;height:35px;">
  Nom <input id="cn" autocomplete="cc-name"><br><br>
      <input name="ao" autocomplete="organization">
      <input name="af" autocomplete="street-address">
      <input name="Pays" autocomplete="country">
</div></td></tr>/table>
```

Lorsque la victime saisit les informations dans le seul champ qu'elle voit, à savoir le Nom, Chrome remplira également (si possible) les autres champs et enverra le tout au serveur, qui aura alors récupéré des données personnelles de la victime.

Contre-mesures

Afin de pallier ce problème, certains navigateurs web ont mis en place quelques mécanismes de protection. Par exemple, certains ne complètent les champs concernant les données bancaires que dans le cas d'une connexion HTTPS. Ceci n'est cependant pas une solution idéale étant donné que le site malveillant peut très bien avoir un certificat valide et donc opérer une connexion SSL. La vraie solution consiste simplement à désactiver cette fonctionnalité dans le navigateur.

- Pour Chrome : Paramètres -> Afficher les paramètres avancés -> sous Mots de passe et formulaires, décocher Activer la saisie automatique.
- Pour Safari : Préférences -> Décocher Saisie automatique
- Pour Opera : Paramètres -> Décocher Saisie automatique

Documentation

- http://thehackernews.com/2017/01/browser-autofill-phishing.html
- https://github.com/anttiviljami/browser-autofill-phishing
- http://blog.elevenpaths.com/2013/10/how-to-take-advantage-of-chrome.html

3 - Rappel des avis émis

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

- CERTFR-2017-AVI-047 : Vulnérabilité dans Xen QEMU
- CERTFR-2017-AVI-048 : Vulnérabilité dans F5 BIG-IP
- CERTFR-2017-AVI-049 : Vulnérabilité dans SCADA Siemens SIMATIC Logon
- CERTFR-2017-AVI-050 : Multiples vulnérabilités dans le noyau Linux SUSE
- CERTFR-2017-AVI-051 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2017-AVI-052 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-053 : Multiples vulnérabilités dans le noyau Linux de SUSE

Gestion détaillée du document

20 février 2017 version initiale.

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-2017-ACT-008