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 31 mars 2015
N° CERTFR-2015-ALE-004-001

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Microsoft Internet Explorer

Gestion du document

Référence	CERTFR-2015-ALE-004
Titre	Vulnérabilité dans Microsoft Internet Explorer
Date de la première version	10 février 2015
Date de la dernière version	31 mars 2015
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- contournement de la politique de sécurité
- injection de code indirecte à distance

2 - Systèmes affectés

- Internet Explorer version 10
- Internet Explorer version 11

3 - Résumé

Une vulnérabilité référencée par l'identifiant CVE-2015-0072, a été découverte dans *Microsoft Internet Explorer*. Elle permet à un attaquant de contourner la politique dite *Same Origin Policy* et d'exécuter du code *JavaScript* malveillant via le chargement d'une page HTML.

3 -.1 Fonctionnement de l'attaque

La politique *SOP* (*Same Origin Policy*) est mise en place pour éviter que des scripts malveillants puissent accéder aux données présentes sur d'autres domaines, notamment aux cookies HTTP permettant de maintenir les sessions authentifiées.

L'exploitation de cette vulnérabilité permet de contourner cette protection et donc d'exécuter du code *JavaScript* dans le contexte d'une page tierce telle qu'une application métier, un site bancaire, ou tout autre application sensible.

3 -.2 Scénarios possibles d'attaque

Cette vulnérabilité est susceptible d'être mise en oeuvre lors de tentatives d'hameçonnage ou lors d'attaques par point d'eau.

3 -.3 Risques encourus

Les risques encourus sont similaires à ceux liés aux attaques de type injection de code indirecte (XSS). En particulier, l'exploitation de cette vulnérabilité peut permettre de récupérer les cookies envoyés par le navigateur pour usurper une session authentifiée.

Se référer à la note d'information CERTA-2002-INF-001-001 pour plus de détails.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Référence CVE CVE-2015-0072
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0072
- Recommandations pour le déploiement sécurisé du navigateur Google Chrome sous Windows
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-pour-le-deploiement-securise-du-navigateur-google-chrome-sous.html
- Recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-pour-le-deploiement-securise-du-navigateur-mozilla-firefox-sous.html
- Universal XSS vulnerability discovered in Microsoft Internet Explorer
  http://www.symantec.com/connect/blogs/universal-xss-vulnerability-discovered-microsoft-internet-explorer
- Mitigating Cross-site Scripting With HTTP-only Cookies
  https://msdn.microsoft.com/en-us/library/ms533046.aspx
- Mitigating framesniffing with the X-Frame-Options header
  https://support.microsoft.com/kb/2694329
- Note d'information : vulnérabilité de type Cross Site Scripting (XSS)
  http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-001/CERTA-2002-INF-001.html
- Bulletin de sécurité Microsoft MS15-018 du 10 Mars 2015
  https://technet.microsoft.com/library/security/ms15-018

Gestion détaillée du document

10 février 2015 version initiale ;

31 mars 2015 fermeture de l'alerte suite à la publication d'un correctif par l'éditeur.