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 juillet 2015
N° CERTFR-2015-ACT-029

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-029

1 - Mise à jour mensuelle Microsoft

Le 14 juillet 2015, Microsoft a publié 14 bulletins de sécurité, dont 4 sont considérés comme critiques et 10 comme importants :

- MS15-065 (critique) qui concerne Internet Explorer ;
- MS15-066 (critique) qui concerne le moteur de script VBScript ;
- MS15-067 (critique) qui concerne l'implémentation du protocole RDP ;
- MS15-068 (critique) qui concerne Hyper-V ;
- MS15-058 (important) qui concerne SQL Server ;
- MS15-069 (important) qui concerne Windows ;
- MS15-070 (important) qui concerne Microsoft Office ;
- MS15-071 (important) qui concerne Netlogon ;
- MS15-072 (important) qui concerne le composant Microsoft Graphics ;
- MS15-073 (important) qui concerne le noyau Windows ;
- MS15-074 (important) qui concerne le service d'installation de Windows;
- MS15-075 (important) qui concerne OLE ;
- MS15-076 (important) qui concerne les appels de procédure distante (RPC) ;
- MS15-077 (important) qui concerne le pilote de polices Adobe Type Manage.

Internet Explorer

Le bulletin cumulatif MS15-065, concernant Internet Explorer, fait état de multiples corruptions mémoire pouvant entraîner une exécution de code arbitraire à distance, ainsi que des vulnérabilités permettant une élévation de privilèges, ou permettant le contournement du mécanisme ASLR (Address Space Layout Randomization, distribution aléatoire de l'espace mémoire). La vulnérabilité CVE-2015-2398 a été divulguée publiquement.

Le bulletin MS15-066 corrige une vulnérabilité dans le moteur de script VBScript qui pourrait permettre une exécution de code arbitraire à distance.

Windows

Le bulletin MS15-069 fait état de deux vulnérabilités dans Microsoft Windows. L'une d'entre elles (vulnérabilité CVE-2015-2368) concerne le gestionnaire de chargement de bibliothèques dynamiques. Un attaquant pourrait l'exploiter via un fichier DLL spécialement formé en incitant un utilisateur à lancer un programme chargeant ce fichier afin de provoquer une exécution de code arbitraire à distance. De la même façon, la seconde vulnérabilité référencée CVE-2015-2369 est provoquée lorsque l'application Windows Media Device Manager charge un fichier DLL malveillant. L'attaquant doit inciter l'utilisateur à ouvrir un fichier RTF.

Le bulletin MS15-077 corrige une vulnérabilité dans le pilote de polices Adobe Type Manage. Cette vulnérabilité permet d'exécuter du code arbitraire.

Le protocole RDP fait l'objet d'une correction dans le bulletin MS15-067 : la vulnérabilité CVE-2015-2373 permet de provoquer un déni de service ou une exécution de code arbitraire. Pour exploiter cette vulnérabilité, l'attaquant doit envoyer des paquets RDP spécialement formés à la victime. A noter que le protocole RDP n'est pas activé par défaut sous Windows.

NETLOGON fait l'objet également d'une correction dans le bulletin MS15-071, la vulnérabilité CVE-2015-2374 associée, peut permettre une élévation de privilèges. Pour exploiter cette vulnérabilité, l'attaquant doit avoir accès à un contrôleur de domaine principal.

Le bulletin MS15-073 fait état de six vulnérabilités corrigées dans le pilote Windows win32k.sys. Ces vulnérabilités peuvent provoquer une élévation de privilèges ou une divulgation d'informations.

Le service d'installation de Windows est également sujet à une correction pour la vulnérabilité CVE-2015-2371, qui permet une élévation de privilèges.

Une élévation de privilèges est également corrigée dans le bulletin MS15-072 pour le composant Windows Graphics. Cette vulnérabilité survient lorsque ce composant échoue à convertir correctement des images de type bitmap.

Une dernière vulnérabilité de type élévation de privilèges est corrigée dans le bulletin MS15-075 pour le composant OLE de Windows.

Office

Le bulletin MS15-070 fait état de huit vulnérabilités. Six d'entre elles permettent l'exécution de code arbitraire à distance dans le contexte de l'utilisateur actif. Cela concerne plusieurs versions de Microsoft Office, de la version 2007 à la version 2013. A noter que certaines de ces exécutions de code arbitraire à distance concernent aussi les visionneuses Microsoft Word et Excel, le pack de compatibilité de Microsoft Office Service Pack 3, les serveurs SharePoint 2010 et 2013.

La vulnérabilité de type corruption mémoire, identifiée CVE-2015-2424, a déjà été observée dans le cadre d'attaques.

Hyper-V

Le bulletin MS15-068 corrige deux vulnérabilités (CVE-2015-2361 et CVE-2015-2362) dans Hyper-v permettant l'exécution de code arbitraire.

SQL Server

Enfin, un dernier bulletin le MS15-058 concerne SQL Server. Il corrige trois vulnérabilités provoquant l'élévation de privilèges ou l'exécution de code arbitraire. Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande de les appliquer dès que possible.

Documentation

- https://technet.microsoft.com/en-us/library/security/MS15-077
- https://technet.microsoft.com/en-us/library/security/MS15-076
- https://technet.microsoft.com/en-us/library/security/MS15-075
- https://technet.microsoft.com/en-us/library/security/MS15-074
- https://technet.microsoft.com/en-us/library/security/MS15-073
- https://technet.microsoft.com/en-us/library/security/MS15-072
- https://technet.microsoft.com/en-us/library/security/MS15-071
- https://technet.microsoft.com/en-us/library/security/MS15-070
- https://technet.microsoft.com/en-us/library/security/MS15-069
- https://technet.microsoft.com/en-us/library/security/MS15-068
- https://technet.microsoft.com/en-us/library/security/MS15-067
- https://technet.microsoft.com/en-us/library/security/MS15-066
- https://technet.microsoft.com/en-us/library/security/MS15-065
- https://technet.microsoft.com/en-us/library/security/MS15-058

2 - URL RFC2397

En 2008, le CERTA décrivait le schéma d'URI « *data://* ». Avec ce type de schéma, le navigateur interprète les données contenues dans l'URI et les affiche. Une URI « *data://* », spécifiée dans la RFC 2397 suit le format suivant :

```
data:[<type>][;codage],<données>
```

Le CERT-FR détecte régulièrement l'utilisation de ce type de schéma d'URI dans des emails de phishing, afin de passer outre la vigilance des utilisateurs. Un attaquant peut en effet insérer dans un email de phishing ce type d'URI :

```
data:text/html;https://www.example.com;base64,PGh0bWw+CiAgIC
A8aGVhZD4KICAgICAgICA8dGl0bGU+UGFnZSBkZSBjb25uZXhpb24gZGUgdm
90cmUgYmFucXVlIEV4YW1wbGUuY29tPC90aXRsZT4KICAgIDwvaGVhZD4KIC
AgIDxib2R5PgogICAgICAgIFJlc3RlIGR1IHNpdGUgV2ViIGRlIGh0dHBzOi
8vd3d3LmV4YW1wbGUuY29tCiAgICA8L2JvZHk+CiA8L2h0bWw+
```

Cet exemple présente à un utilisateur non averti une adresse contenant « *https://www.example.com* », qui pourrait être l'adresse du site de sa banque.

Un navigateur qui ouvre ce lien décodera la chaîne au format Base64 « *PGh0bWw+Ci ...* », qui correspond au message suivant :

```
<html>
    <head>
        <title>Page de connexion de votre banque Example.com</title>
    </head>
    <body>
        Reste du site Web de https://www.example.com
    </body>
</html>
```

Cet exemple trivial peut être remplacé par le code HTML complet copiant la page de connexion d'un site bancaire, mais qui transmettra les identifiants renseignés par la victime à l'attaquant.

Toutefois, dans ce cas, le navigateur ne présentera pas de visuel indiquant que la page présentée a été téléchargée depuis un serveur implémentant TLS avec un certificat valide, ce qui n'est le plus souvent pas le cas de la page de connexion légitime.

Certaines extensions, comme NoScript pour FireFox, bloquent ce type d'URI par défaut.

Documentation

- Bulletin d'actualité CERTFR-2008-ACT-047 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2008-ACT-047/
- Description de la RFC2397 :
  https://www.ietf.org/rfc/rfc2397.txt
- Noscript :
  https://noscript.net

3 - Rappel des avis émis

Dans la période du 13 au 18 juillet 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-ALE-007 : Vulnérabilité dans Oracle Java SE
- CERTFR-2015-AVI-288 : Multiples vulnérabilités dans Moodle
- CERTFR-2015-AVI-289 : Multiples vulnérabilités dans Microsoft SQL Server
- CERTFR-2015-AVI-290 : Vulnérabilité dans le pilote de police Adobe Type Manager
- CERTFR-2015-AVI-291 : Vulnérabilité dans Microsoft Remote Procedure Call
- CERTFR-2015-AVI-292 : Multiples vulnérabilités dans Microsoft Windows OLE
- CERTFR-2015-AVI-293 : Vulnérabilité dans le service d'installation de Windows

– CERTFR-2015-AVI-294 : Multiples vulnérabilités dans le noyau Windows
– CERTFR-2015-AVI-295 : Vulnérabilité dans le composant Microsoft Graphics
– CERTFR-2015-AVI-296 : Vulnérabilité dans Microsoft Netlogon
– CERTFR-2015-AVI-297 : Multiples vulnérabilités dans Microsoft Office
– CERTFR-2015-AVI-298 : Multiples vulnérabilités dans Microsoft Windows
– CERTFR-2015-AVI-299 : Multiples vulnérabilités dans Microsoft Hyper-v
– CERTFR-2015-AVI-300 : Vulnérabilité dans Microsoft RDP
– CERTFR-2015-AVI-301 : Vulnérabilité dans le moteur de script VBscript
– CERTFR-2015-AVI-302 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTFR-2015-AVI-303 : Multiples vulnérabilités dans Oracle Database Server
– CERTFR-2015-AVI-304 : Multiples vulnérabilités dans Oracle MySQL
– CERTFR-2015-AVI-305 : Multiples vulnérabilités dans Oracle Java SE
– CERTFR-2015-AVI-306 : Multiples vulnérabilités dans Oracle Sun Systems
– CERTFR-2015-AVI-307 : Multiples vulnérabilités dans Oracle Berkeley DB
– CERTFR-2015-AVI-308 : Multiples vulnérabilités dans Oracle Solaris
– CERTFR-2015-AVI-309 : Multiples vulnérabilités dans Adobe Flash Player
– CERTFR-2015-AVI-310 : Multiples vulnérabilités dans Adobe Shockwave Player
– CERTFR-2015-AVI-311 : Vulnérabilité dans le noyau Linux Red Hat

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2015-ALE-006-001 : Vulnérabilité dans Adobe Flash Player (rajout de la vulnérabilité CVE-2015-5123.)
– CERTFR-2015-ALE-006-001 : Vulnérabilité dans Adobe Flash Player (rajout de la vulnérabilité CVE-2015-5123.)

Gestion détaillée du document

20 juillet 2015 version initiale.