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 19 septembre 2016
N° CERTFR-2016-ACT-038

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-038

1 - WPAD et conflits de nommage

Une équipe de chercheur a publié [1] les détails d'une étude montrant que des requêtes DNS, normalement destinées à des serveurs DNS internes d'entreprise, atteignent par erreur des serveurs DNS Racine publics. Les requêtes DNS en question sont liées au protocole *Web Proxy Auto-Discovery* (WPAD). Des acteurs malveillants pourraient profiter de ce phénomène et de l'introduction de nouveaux noms de domaine de premier niveau génériques (*new gTLDs*) [4] pour effectuer des attaques de type « homme au milieu » (*MitM*).

Aperçu de WPAD

Le protocole *Web Proxy Auto-Discovery* (WPAD) permet à un système de localiser automatiquement un fichier de configuration de serveur mandataire (*proxy*). Ce protocole, notamment supporté et activé par défaut dans *Internet Explorer* sous Windows, est principalement utilisé dans les réseaux internes d'entreprise. La façon dont le fichier de configuration est récupéré est critique. Si un attaquant parvient à fournir son propre fichier de configuration à des clients, il peut alors se placer en position de MitM et ainsi surveiller ou modifier les communications qui transitent par son serveur mandataire. Par défaut, le fichier de configuration, nommé `wpad.dat`, est localisé en essayant successivement les méthodes suivantes :

1. requête DHCP ;
2. requête DNS ;
3. requête *Link-Local Multicast Name Resolution* (LLMNR) ;
4. requête *NetBios*.

Cet article s'intéresse à la méthode DNS, utilisée lorsque la requête DHCP est sans réponses. L'URL du fichier de configuration est alors déduite grâce au nom du domaine dans lequel se trouve la machine. Par exemple, si une machine se trouve dans le réseau d'une entreprise dont le domaine interne est `entreprise.exemple`, l'URL déduite sera `http://wpad.entreprise.exemple/wpad.dat`. Une requête DNS est alors effectuée pour résoudre `wpad.entreprise.exemple`.

Risque : conflit de nommage

La requête DNS de WPAD est normalement destinée à un serveur DNS interne de l'entreprise. Toutefois, il arrive qu'une telle requête atteigne un serveur DNS racine publique. Cette situation, pouvant se produire à cause d'une mauvaise configuration ou lorsqu'un employé connecte un appareil professionnel sur son réseau domestique, porte le nom de conflit de nommage (*name collision*) [3]. Ce conflit peut mener à des résultats inattendus, voire malveillants. Dans notre exemple, le nom de domaine de premier niveau (TLD) `.exemple` ne fait pas partie de ceux enregistrables publiquement (RFC 2606 [5]). Un serveur DNS Racine public ne saura donc pas répondre et le résultat est a priori sans risque.

En revanche, si l'entreprise avait choisi un TLD existant également publiquement, comme `.com`, alors n'importe qui aurait pu enregistrer le sous-domaine correspondant et se faire passer pour le serveur hébergeant le fichier WPAD.

D'après l'article [1], en observant les requêtes envoyées à 2 des 13 serveurs DNS racine, environ 20 millions de requêtes WPAD les atteignent chaque jour.

Facteur aggravant : *new gTLDs*

L'apparition, relativement récente, de nouveaux noms de domaines de premier niveau génériques (*new gTLDs* [4]) accentue les risques liés au conflit de nommage. Voici des exemples de gTLD qui auraient pu être choisis pour le nommage du réseau interne d'une entreprise, mais sont maintenant enregistrables publiquement :

- `.group`
- `.network`
- `.dev`
- `.office`
- `.global`
- `.ads`

Recommandations

Le CERT-FR recommande :

- la désactivation de WPAD s'il n'est pas utilisé ;
- d'utiliser un nom de domaine enregistré publiquement et sous le contrôle de l'entreprise comme nom racine pour le nommage du réseau interne ;
- configurer les serveurs mandataires ou pare-feu pour journaliser et bloquer les requêtes WPAD sortantes.

Documentation

1 Verisign, *MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era* :
http://www.verisign.com/assets/labs/MitM-Attack-by-Name-Collision-Cause-Analysis-and-WPAD-Vulnerability-Assessment-in-the-New-gTLD-Era.pdf

2 Alerte de l'US-CERT TA16-144A, *WPAD Name Collision Vulnerability* :
https://www.us-cert.gov/ncas/alerts/TA16-144A

3 Conflit de nommage :
https://www.icann.org/resources/pages/name-collision-2013-12-06-en

4 Nouveaux noms de domaine de premier niveau génériques (gTLD) :
https://newgtlds.icann.org/en/about/program

5 RFC 2606, *Reserved Top Level DNS Name* :
https://tools.ietf.org/html/rfc2606

2 - Mise à jour mensuelle de Microsoft

Le 13 septembre, lors de sa mise à jour mensuelle, Microsoft a publié quatorze bulletins de sécurité, dont sept sont considérés comme critiques et sept comme importants :

- MS16-104 (critique) concernant Internet Explorer ;
- MS16-105 (critique) concernant le navigateur Edge ;
- MS16-106 (critique) concernant le composant Microsoft Graphics ;
- MS16-107 (critique) concernant Microsoft Office ;
- MS16-108 (critique) concernant Microsoft Exchange Server ;
- MS16-116 (critique) concernant OLE Automation pour le moteur de script VBScript :
- MS16-117 (critique) concernant Adobe Flash Player :
- MS16-109 (important) concernant Silverlight :
- MS16-110 (important) concernant Microsoft Windows :
- MS16-111 (important) concernant le noyau Windows :
- MS16-112 (important) concernant l'écran de verrouillage Windows :
- MS16-113 (important) concernant le mode de noyau sécurisé de Windows :
- MS16-114 (important) concernant pour serveur SMBv1 Windows :
- MS16-115 (important) concernant la bibliothèque PDF Microsoft Windows :

Navigateurs

Cette mise à jour corrige dix vulnérabilités dans Internet Explorer. Cinq permettent une exécution de code à distance et deux d'entre elles sont considérées comme critiques. La vulnérabilité CVE-2016-3295 est déclenchée par une corruption de mémoire dans le navigateur. La vulnérabilité CVE-2016-3375 est due à une possible altération de mémoire dans de moteur de script. Deux mises à jour sont nécessaires pour combler cette dernière vulnérabilité : celle concernant Internet Explorer et celle concernant le mécanisme Microsoft OLE Automation pour le moteur de script VBScript. Les trois autres vulnérabilités permettant une exécution de code à distance ont un impact moindre et sont également causées par des corruptions potentielles de la mémoire à cause de la manière dont Internet Explorer traite les objets en mémoire.

La vulnérabilité CVE-2016-3292 permet un échappement de bac à sable, débouchant sur une élévation de privilèges.
Trois vulnérabilités sont de type divulgation d'informations. Les vulnérabilités CVE-2016-3325 et CVE-2016-3351 proviennent de la manière dont Internet Explorer traite les objets en mémoire. Microsoft indique que cette dernière est activement exploitée. La vulnérabilité CVE-2016-3291 est causée par le traitement des requêtes trans-origines (cross-origin requests) et pourrait permettre à un attaquant de découvrir l'origine de toutes les pages internet dans un navigateur. La vulnérabilité CVE-2016-3353 permet un contournement de la politique de sécurité et est corrigée en changeant la manière dont Internet Explorer traite les fichiers .URL. Douze vulnérabilités ont été corrigées dans Microsoft Edge. Sept permettent une exécution de code à distance et les cinq autres une fuite d'information.
Parmi les vulnérabilités permettant une exécution de code à distance, quatre sont considérées critiques. Les vulnérabilités CVE-2016-3294 et CVE-2016-3295 peuvent être causées par une corruption de mémoire dans le navigateur. Les vulnérabilités CVE-2016-3350 et CVE-2016-3377 impactent le moteur Chakra JavaScript.
La vulnérabilité CVE-2016-3391 impacte Edge tout comme Internet Explorer. Les quatre autres vulnérabilités permettant une fuite d'informations proviennent de la manière dont certaines fonctions traitent les objets en mémoire.

Dans son bulletin MS16-117, Microsoft reprend les 29 vulnérabilités décrites par Adobe dans son bulletin de sécurité APSB16-29 concernant son Flash Player. 26 de ces vulnérabilités permettent une exécution de code à distance et impactent le greffon Flash Player d'Internet Explorer et d'Edge.

Bureautique

Treize vulnérabilités sont corrigées dans la suite bureautique Office. Dix d'entre elles permettent une exécution de code à distance, dont la vulnérabilité CVE-2016-3357, qui est jugée critique. Elles sont toutes dues à de possibles altérations de mémoire.
La vulnérabilité CVE-2016-0137 impacte la manière dont les composants 'Démarrer en un clic'(C2R) traitent les objets en mémoire, ce qui peut permettre un contournement de la distribution aléatoire de l'espace d'adressage (ASLR).
La vulnérabilité CVE-2016-0141 permet à un attaquant de récupérer la clé privée d'un utilisateur. En effet, une macro Visual Basic dans Office peut exporter celle-ci de manière incorrecte lors de l'enregistrement d'un document.
La vulnérabilité CVE-2016-3366 provient du fait que Microsoft Outlook ne respecte pas strictement la RFC 2046. De ce fait, Outlook peut identifier de manière incorrecte la fin d'une pièce jointe de type MIME, ce qui peut entraîner un dysfonctionnement au niveau d'une analyse antivirus ou anti-spam.

Windows

La vulnérabilité CVE-2016-3356 touche le composant Microsoft Graphics. Celle-ci est jugée critique dans le contexte de Windows 10 et peut permettre une exécution de code à distance.
La vulnérabilité CVE-2016-3354 permet une fuite d'informations à cause de la manière dont l'interface Windows Grapics Device Interface (GDI) traite les adresses mémoire.
Trois vulnérabilités d'élévations impactant les composants graphiques de Windows ont été corrigées, deux dans Win32k (CVE-2016-3348 et CVE-2016-3349) et une dans GDI (CVE-2016-3355). Évoquée dans la section Navigateurs, la vulnérabilité CVE-2016-3375 permet une exécution de code à distance et est jugée critique. Elle provient d'une possible altération de mémoire due à la manière dont le mécanisme Microsoft OLE Automation et le moteur de script VBScript dans Internet Explorer accèdent aux objets en mémoire. Cinq vulnérabilités d'élévation de privilèges sont réparées dans le noyau de Windows.
La vulnérabilité CVE-2016-3302 permet une élévation de privilèges, car Windows autorise de manière incorrecte le chargement de contenu internet à partir de l'écran de verrouillage.

La vulnérabilité CVE-2016-3344 peut déboucher sur une fuite d'information au niveau du mode de noyau sécurisé de Windows.
Deux vulnérabilités de divulgation d'informations impactent la bibliothèque PDF dans Windows et pourraient permettre à un attaquant d'obtenir des données sensibles dans le but de compromettre le système.
De manière plus générale, quatre autres vulnérabilités sont corrigées dans Windows. La première (CVE-2016-3346) concerne une élévation de privilèges rendue possible par le chargement d'un fichier DLL piégé. La deuxième (CVE-2016-3368) peut déboucher sur une exécution de code à distance jugée importante. La troisième (CVE-2016-3369) peut engendrer un déni de service. La vulnérabilité CVE-2016-3352 permet à un attaquant d'abuser les demandes d'authentification unique (SSO) NT Lan Manager (NTLM) pendant une ouverture de session avec un compte Microsoft (MSA). Il peut ensuite récupérer un condensé cryptographique du mot de passe NTLM afin de tenter de le deviner par force brute. Microsoft note que la vulnérabilité CVE-2016-3352 a été révélée publiquement. La vulnérabilité CVE-2016-3345 permet une exécution de code à distance sur un serveur Microsoft Server Message Block 1.0 (SMBv1) sur des systèmes antérieurs à Windows 8.1 grâce à des requêtes mal formées. Sur des systèmes plus récents, l'impact est limité à un déni de service. Microsoft indique également que pour que cette vulnérabilité soit exploitée, l'attaquant doit être authentifié sur le serveur et être autorisé à ouvrir des fichiers.
Plusieurs vulnérabilités ont été corrigées dans Microsoft Exchange Server. Sont concernées une vulnérabilité de divulgation d'informations (CVE-2016-0138), une vulnérabilité de redirection ouverte (CVE-2016-3378) et une vulnérabilité d'élévation de privilèges (CVE-2016-3379). De plus, ce correctif répare de nombreuses vulnérabilités dans les bibliothèques Oracle Outside In : 11 vulnérabilités permettant une exécution de code à distance, une vulnérabilité de divulgations d'informations et six vulnérabilités pouvant déboucher sur un déni de service. Ces vulnérabilités avaient été corrigées par Oracle à l'occasion de son bulletin de juillet 2016. Enfin, l'application Micosoft Silverlight a reçu un correctif pour la vulnérabilité CVE-2016-3367, notée importante et permettant une exécution de code à distance.

Recommandations

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

3 - Rappel des avis émis

Dans la période du 12 au 18 septembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-304 : Vulnérabilité dans Moodle
- CERTFR-2016-AVI-305 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-306 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2016-AVI-307 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-308 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-309 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-310 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-311 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-312 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-313 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-314 : Vulnérabilité dans Citrix Linux VDA

Gestion détaillée du document

19 septembre 2016 version initiale.