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 28 novembre 2016
N° CERTFR-2016-ACT-048

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-048

1 - Risques liées aux relations de confiance entre services Web

Le 18 novembre 2016, un certain nombre de comptes Twitter à forte audience ont diffusé des messages incitant les internautes à cliquer sur un lien dans l'objectif de les rediriger vers un service proposant l'acquisition de nouveaux abonnés (followers).

Ces Tweets n'ont pas été postés de manière délibérée par les personnes possédant ces différents comptes. Il ne sont pas non plus le résultat d'une éventuelle compromission du compte via l'interception ou le vol d'informations d'authentification.

Les personnes malveillantes à l'origine de ces Tweets ont simplement tiré parti de la relation de confiance établie entre les différents comptes Twitter en question et une application compromise d'une société tierce, que l'utilisateur avait autorisée d'interagir avec son compte.

Twitter, comme un certain nombre d'outils, offre la possibilité à des développeurs de pouvoir interagir avec leur contenu, via la création d'applications basées sur l'utilisation d'une interface de programmation (API). Afin que l'utilisateur ne soit pas dans l'obligation de fournir ces informations de connexion au service Twitter (identifiant et mot de passe) à chacune de ces applications, un système de délégation d'autorisation est mis en place par l'intermédiaire du protocole libre OAuth. Les spécifications liées à ce protocole sont définies, pour ce qui est de la version 2.0, dans les RFCs 6749 et 6750. Ce protocole permet ainsi à une application de pouvoir interagir avec un service pour le compte d'un utilisateur à l'aide d'un simple jeton d'authentification, à condition que cet accès ait été préalablement autorisé par l'utilisateur.

Un nombre conséquent d'applications est concerné, notamment des outils de veille, de statistiques, de gestion des favoris, de raccourci d'URL ou bien encore d'applications mobiles. Il est possible à tout moment de visualiser la liste des applications ayant accès à un compte Twitter en se rendant dans la partie «Paramètres» du compte puis dans «Applications». L'ensemble des applications auxquelles l'utilisateur a décidé de faire confiance y est ainsi repris. Il est possible de révoquer l'accès de chacune d'entres-elles à tout moment. Il est intéressant de noter que lorsqu'un utilisateur décide d'autoriser une application à interagir avec son compte, les différentes permissions que l'utilisateur accordera à cette dernière sont présentées à l'utilisateur. Celles-ci doivent donc être analysées avec précaution. Ces permissions peuvent être un simple accès en lecture aux messages du fil de l'utilisateur. D'autres permissions peuvent s'avérer davantage problématiques en cas de compromission de l'application, telles que la possibilité de pouvoir poster des messages en lieu et place de l'utilisateur. La liste exhaustive des permissions auxquelles une application peut avoir accès est décrite au sein de la documentation développeur.

Le cas évoqué ici est lié à l'outil Twitter, mais les préconisations s'appliquent de manière générale à toute relation de confiance entre services Webs. Ainsi, il est important d'avoir à l'esprit que lorsqu'un utilisateur octroie des permissions à une application concernant l'accès à un service, la sécurité de ce service ne repose donc plus uniquement sur l'utilisateur (par la capacité à garder ces identifiants secrets) et la personne mettant ce service à disposition (par la capacité à sécuriser le service et donc le contenu de l'utilisateur), mais devient de fait dépendante également de la sécurité de l'application tierce. Par conséquent, si un utilisateur autorise des dizaines d'applications à pouvoir interagir en son nom auprès d'un service, la compromission par une personne mal intentionnée d'une seule de ces applications suffit à mettre à mal la sécurité du contenu lié à l'utilisateur. Il est important

de noter que la compromission d'une application, dans le cas où un système de délégation de droit comme celui évoqué précédemment est utilisé, ne remet pas en cause les informations d'authentification de l'utilisateur, mais uniquement le jeton d'authentification utilisé entre l'application et le service. Cependant, il n'est pas impossible que l'application demande à l'utilisateur des informations personnelles telles qu'une adresse de courriel pour lui envoyer des notifications ou des informations par exemple. Dans ce cas, une compromission de l'application peut entraîner un accès à des données qui ne sont pas directement liées au service. Enfin, il est intéressant de rappeler ici les bonnes pratiques concernant la gestion des mots de passe et notamment le fait d'utiliser un mot de passe unique pour chaque service utilisé.

Documentation

- RFC 6749 :
  https://tools.ietf.org/html/rfc6749
- RFC 6750 :
  https://tools.ietf.org/html/rfc6750
- Gestion des applications Twitter :
  https://support.twitter.com/articles/96224
- Documentation développeur permettant de lister les interactions possible avec un compte Twitter :
  https://dev.twitter.com/rest/reference
- Sécurité des mots de passe :
  https://www.ssi.gouv.fr/guide/mot-de-passe/

2 - Rappel des avis émis

Dans la période du 21 au 27 novembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-385 : Multiples vulnérabilités dans Moodle
- CERTFR-2016-AVI-386 : Vulnérabilité dans Nagios
- CERTFR-2016-AVI-387 : Multiples vulnérabilités dans Xen
- CERTFR-2016-AVI-388 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-389 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2016-AVI-390 : Multiples vulnérabilités dans phpMyAdmin

Gestion détaillée du document

28 novembre 2016 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-2016-ACT-048`