SECURISER LES LOGICIELS SAS 9.4 ACCESSIBLES PAR LE WEB

Caractéristiques :

Catégories : SAS Foundation, SAS/CONNECT, SAS Metadata Server, SAS Web Server, SAS Web Application Server

OS : Windows, Unix

Version : SAS® 9.4

Vérifié en septembre 2016

A l'heure où de plus en plus d'applications SAS (comme Visual Analytics) sont disponibles en tant que services sur l'internet, il est indispensable de considérer leur sécurisation comme une priorité.

A l'heure où l'économie numérique est en plein essor, les systèmes informatiques sont la proie de cybercriminels munis d'outils très perfectionnés et évoluant sans cesse. La recherche universitaire découvre également régulièrement des vulnérabilités dans les logiciels qui composent les standards de l'industrie tels que Java, OpenSSL, Spring, Apache.

La prise en compte de la sécurité des logiciels est donc devenue incontournable.

Sommaire

1. STANDARDS DE L'INDUSTRIE LOGICIELLE ET VULNERABILITES CONNUES

1.1. Architecture des logiciels dans l'industrie

Les éditeurs de logiciels, dont SAS, concentrent leurs efforts pour développer de manière continue les fonctionnalités, les performances et la qualité des produits pour lesquels leur expertise est reconnue.

Afin de rendre les systèmes d'information interopérables et dans le but de raccourcir les cycles de développement, la grande majorité des éditeurs s'appuie généralement sur des technologies tierces qui se sont au fil du temps imposées comme des standards de l'industrie grâce à leur souplesse, leurs performances, flexibilité et nombreuses fonctionnalités.

Ceci présente de nombreux avantages pour l'éditeur de logiciels:

- ne pas avoir à réécrire des modules « socles » de tout logiciel, par exemple des modules de communication, d'authentification, de gestion d'applications et de mémoire, d'accès aux bases de données … etc.
- de permettre aux administrateurs et développeurs d'avoir moins de systèmes hétérogènes à maintenir et de mutualiser leurs compétences d'un système à l'autre.

Ces composants tierces parties sont généralement développés par d'autres éditeurs, des fondations à but non lucratif ou des organisations Open Source…

Les logiciels SAS utilisent notamment les technologies suivantes :

- **Java** :

Java est l'environnement d'exécution et développement d'applications le plus répandu dans le monde à ce jour.
Cet environnement est très riche en fonctionnalités (authentification, de gestion d'applications web, accès aux bases de données, développement d'applications…). Il s'agit du choix technique de SAS pour l'exécution de ses applications Web, telles que SAS Enterprise BI Server, SAS Enterprise Miner, SAS Visual Analytics & Visual Statistics, SAS Marketing Automation…

L'environnement Java a été initialement créé par la société Sun, depuis lors, acquise par Oracle.

- **Apache**

Apache est une fondation à but non lucratif spécialisée dans l'édition de nombreux « frameworks » (ensemble de fonctionnalités) utilisés par les technologies du Web.
Ces technologies sont sous licence OpenSource.

Apache Software Fundation est à l'origine notamment du fameux **Apache Web Server**, du serveur d'applications Java **Tomcat**, de la suite bureautique open source : Apache **OpenOffice**, ainsi que de la suite logicielle **Hadoop**, qui s'appuie sur **HDFS**, **Hive**, **Spark, YARN, Impala**…

- **OpenSSL**

OpenSSL est un autre projet OpenSource, qui implémente le cryptage des communications entre un terminal et un serveur.
Cette technologie est un standard du web et est utilisée à chaque fois que vous accédez à une adresse internet (URL) qui commence par « https » (un cadenas apparaît dans votre navigateur).

1.2. Position dominante et cybercriminalité

Du fait de leur position prépondérante sur le marché, ces technologies sont très étudiées et sont régulièrement éprouvées par des attaques toujours plus élaborées et complexes.
Il s'en suit une lutte permanente pour les éditeurs de ces technologies palier les failles au fur et à mesure de leurs découvertes, et pour assurer un niveau de sécurité et de fiabilité maximal pour leurs nombreux utilisateurs.
A charge ensuite aux consommateurs de ces technologies (éditeurs entre autres) de mettre à disposition de leurs clients et utilisateurs des correctifs adaptés.

Ces technologies sont très étudiées par les universités, écoles d'ingénieurs, les « hackers », mais aussi des organisations criminelles, partout dans le monde dans le but de dérober des informations ou de se faire passer pour un tiers de confiance.

Tout système d'informations placé dans la zone internet est donc potentiellement la proie d'attaquants localisés dans le monde entier.

1.3. Détail des vulnérabilités listées dans cet article

Vous trouverez ci-dessous une explication des failles connues et des répercussions possibles en cas d'exploitation par un tiers mal intentionné.

Deux « briques logicielles » regroupent presque l'ensemble des vulnérabilités référencées chez SAS :

OpenSSL

OpenSSL est un module logiciel qui permet de crypter des communications entre applications (et de les décrypter).
C'est la technologie qui est derrière le protocole HTTPS fréquemment utilisé sur Internet pour protéger la confidentialité de nos mots de passe, accès banque en ligne, …

Les vulnérabilités identifiées sur OpenSSL permettent potentiellement à des attaquants de « casser » l'algorithme de cryptage utilisé et ainsi de décoder les communications cryptées entre deux points (utilisateur et serveur par exemple) et de s'intercaler entre, en faisant croire aux deux points qu'il est l'autre.
Cette attaque porte le nom de « man in the middle ».

Des mises à jour régulières du module OpenSSL permet de combler les vulnérabilités identifiées.

La plupart des vulnérabilités pouvant potentiellement affecter les logiciels SAS sont liées à OpenSSL : FREAK, SKIP-TLS, POODLE, DROWN, GHOST

Java

Java est un environnement d'exécution d'applications qui peut utiliser la cryptographie et communiquer avec des systèmes utilisant OpenSSL.
Il est donc nécessaire de procéder à des mises à jour de Java afin de combler les vulnérabilités liées à la sécurisation des communications, citées ci-dessus.

Java est également vulnérable à une attaque permettant à un tiers d'exécuter du code Java à distance en exploitant la faille « Java deserialization ».
Cela permet de détourner le comportement du logiciel compromis.
Des composants fournis pas Apache Software Fundation (largement répandus dans le monde logiciel, dont SAS) ont été concernés par cette faille.
L'application des correctifs pour les logiciels SAS est donc très recommandée.

2. REPONSES DE SAS SUR LES VULNERABILITES CONNUES

De nos jours, un certain nombre de dispositifs de sécurité existent et limitent le risque d'intrusions non souhaitées dans les entreprises.
Néanmoins, cela permet de réduire la portée des systèmes compromis.
Afin d'éviter le vol d'informations sur les serveurs accessibles depuis Internet, il est recommandé de mettre à jour les logiciels SAS (essentiellement les serveurs) visibles depuis l'Internet.

SAS communique sur son engagement à fournir des correctifs pour chacune des vulnérabilités touchant ses logiciels.

Ce chapitre présentera les différentes vulnérabilités connues et adressées par SAS afin de répondre aux préoccupations des départements IT en termes de protection des données.

2.1. Vérifier quels correctifs sont nécessaires

SAS intègre les correctifs de sécurité dans certaines révisions du dépôt d'installation.
Cette procédure s'adresse donc aux systèmes SAS ayant été installés avant juin 2016.

Veuillez vérifier le numéro de révision du dépôt SAS.
Cette information est située dans le fichier
<SAS Software Depot>\install_doc\<numero de commande>\soi.html

---

Information for Tech Support Site [redacted]:

Site Name:	SAS INTERNAL 940 16W08 WX6[redacted]
Tech Support Site Number:	[redacted]
Contracts Site Number:	[redacted]
Operating System:	Microsoft® Windows® Server & Workstation for x64
Internal Reference:	SAS 9.4 TS1M3, Rev. 940_16w08

Selon la révision de votre dépôt (année_semaine) et le niveau de maintenance de SAS (par exemple 9.4 TS1M2, 9.4 TS1M3), il vous faut passer en revue les différentes vulnérabilités listées dans le bulletin suivant pour voir quels correctifs sont à installer:

https://support.sas.com/security/alerts.html

Prenons l'exemple suivant :

- Le système SAS installé est en version 9.4 TS1M3 sous Linux
  La révision du dépôt d'installation est :15w33 (i.e. année 2015, semaine 33)

1) La vulnéraribilité FREAK & SKIP-TLS :

- SAS 9.4 TS1M3 inclue déjà ce correctif nativement, il n'est donc pas possible de l'installer.
- Il faut installer la mise à jour du SAS Private Java Runtime Environment sur chaque machine disposant de logiciels SAS.

2) Vulnérabilité DROWN :

- Correctif V53003 à installer pour SAS 9.4 TS1M3. Ce correctif est disponible sur demande auprès du Support SAS.
- Les modifications du protocole SSL à faire sur le SAS Web Server et SAS Web Application Server sont déjà faites lors de l'installation si le dépôt est supérieur à la révision 14w47.

3) Java Deserialization :

- Il faut installer en premier le correctif nommé : sas-security-update-2016-02.zip disponible ici : http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html
  Sauf, si le dépôt est plus récent que la version 16w17, qui l'intègre.

- Il faut ensuite installer le correctif : Y09002 : « supplemental hot fix for SAS Security Update 2016-02).
  Ce correctif est automatiquement inclus dans les dépôts SAS depuis la version du 28 avril 2016

- Il faut également installer le correctif V77007 sur le serveur Web de SAS si la version est TS1M3. Des correctifs sont disponibles pour les maintenances inférieures.

4) Vulnérabilité GHOST

- Cette dernière concerne les machines munies de Linux avec une ancienne version d'un package « glibc ». Une simple mise à jour de ce module linux suffit pour combler cette faille.

5) POODLE

- Cette vulnérabilité liée à openSSL est corrigée dans la version SAS 9.4 TS1M3.

6) BASH

- Une mise à jour du package « bash » sous Linux suffit pour combler cette vulnérabilité

7) Heartbleed
   Cette vulnérabilité est ancienne et a déjà été corrigée par une mise à jour de SAS.
   En optant pour 9.4 TS1M3 avec le correctif pour la faille FREAK (point 1), vous êtes protégés.

2.2. Appliquer les correctifs

Avant de procéder à l'installation des correctifs, veuillez :

- Lire le bulletin et les documentations des correctifs car il y a un ordre à respecter
- Faire une sauvegarde après avoir arrêté les services du système SAS qui sera mis à jour

- Lire les documentations d'installation de chacun des correctifs car certains nécessitent des étapes manuelles pour procéder à leur complète activation.
- Ne pas cocher l'option « configurer » dans le setup des correctifs de sécurité.

Si votre système SAS est réparti sur plusieurs Serveurs :

- Metadata Server & SAS Computation Server
- Middle Tier
- Client Tier

Alors, vous devrez installer les correctifs de sécurité sur chacune des machines de votre déploiement SAS afin de garantir un niveau de sécurité optimal.

2.2.1. Bien respecter l'ordre d'application des correctifs

Le seul correctif SAS nécessitant un ordre particulier concerne la correction de la vulnérabilité « Java Deserialization ».

Il faut en effet, tel que décrit dans la documentation en ligne, installer les modules dans l'ordre suivant :

1) sas-security-update-2016-02.zip
2) Y09002 et V77007
3) Java Runtime 1.7.0_101

Le non-respect de cet ordre entrainera un remplacement des fichiers corrigés par des fichiers vulnérables.

3. EN CAS DE PROBLEME

3.1. Les problèmes les plus fréquents

La variété de l'offre logicielle de SAS ainsi que les différents types de déploiements de logiciels SAS peuvent rendre l'identification des correctifs à appliquer complexe de prime abord.
N'hésitez pas à solliciter le Support Clients SAS en décrivant bien l'architecture et la répartition des « tiers » SAS, ainsi qu'en précisant la version (9.4 TS1M3 par exemple) et la révision du Dépôt qui a servi à faire l'installation. Nous vous aiderons alors à identifier les correctifs nécessaires sur votre environnement.

3.2. Eléments à transmettre au Support Clients

Si vous rencontrez des problèmes lors de l'identification des correctifs à installer ou lors du déploiement de ceux-ci, vous pouvez nous écrire à support@sas.com en joignant à votre message l'erreur reçue.

4. LIENS UTILES

SAS Security Bulletin : Ce dernier est mis à jour régulièrement en fonction des nouvelles vulnérabilités découvertes :
https://support.sas.com/security/alerts.html

Dictionnaire des vulnérabilités (en Anglais), concerne toutes les technologies, même celles non utilisées par SAS:
https://cve.mitre.org/

5. CONCLUSION

La mutation du monde de l'entreprise, des communications, des services proposés sur Internet conjuguée à une économie très concurrentielle sont une manne pour différents acteurs mal intentionnés.

Les moyens de sécurité ne cessent d'évoluer et de se complexifier, mais c'est également le cas des attaques contre ces mêmes systèmes, qui ne cessent d'évoluer en sophistication.

A ce jour, les crimes numériques sont difficiles à détecter et à démontrer devant la justice.
La majorité d'entre eux peuvent être évités en optant pour une mise à jour régulière des logiciels et en adoptant une politique de sécurité rigoureuse (architecture sécurisée, HTTPS, Firewalls) si votre système SAS est disponible depuis l'Internet.

Marc AVEZAC
Consultant Support Clients SAS France