Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 08 février 2013
N° CERTA-2013-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-006

1 Oracle Java version 7 mise à jour 13 - Point de situation

Le 10 janvier 2013, un code d'exploitation a été diffusé publiquement sur internet. Il profite de deux vulnérabilités pour désactiver le gestionnaire de sécurité (Security Manager) de Java (CERTA-2013-ALE-001) :

- la première vulnérabilité permet d'utiliser la méthode `findClass` de la classe `MBeanInstantiator`. Elle permet de charger une classe dans l'espace de noms (*namespace*) système ;
- la deuxième vulnérabilité concerne la nouvelle API `Reflection` de Oracle Java. Cette API est disponible à partir de la version 1.7 du produit. La vulnérabilité découle d'un défaut de vérification lors d'un appel de méthode via l'API. Cette vulnérabilité est utilisée pour appeler des méthodes des classes qui ont été chargées via la première vulnérabilité.

Ces vulnérabilités sont utilisées pour désactiver la *sandbox* Java (*Security Manager*) afin d'exécuter du code arbitraire à distance. Le *Security Manager* est activé sous certaines conditions dans Java. Par exemple lorsque l'on charge une *applet* Java dans un navigateur Web, un *Security Manager* est instancié pour « cloisonner » le plugin Java dans le navigateur. Lorsqu'un attaquant peut désactiver le *Security Manager* d'une *applet* Java, il est capable d'exécuter du code sans restriction de la sandbox sur le client qui consulte la page Web. L'exécution de code est possible avec les droits du processus Java qui exécute l'*applet*.

Le 15 janvier 2013, Oracle a publié la version 7 mise à jour 11 de Java (cf. CERTA-2013-AVI-092). Il s'agit d'une mise à jour « hors cycle » de Oracle qui corrige la deuxième vulnérabilité. Des vérifications ont été ajoutées dans l'API `Reflection`. Il n'est donc plus possible d'utiliser la deuxième vulnérabilité pour appeler des méthodes sur les classes dans l'espace de noms système. L'exploitation des vulnérabilités n'est donc pas fonctionnelle sur la version Java 7 mise à jour 11. Il est toutefois toujours possible d'utiliser la première vulnérabilité dans une *applet* pour charger des classes dans l'espace de noms système. La mise à jour de Java 1.7.11 a augmenté le niveau de sécurité des *applets* Java et des applications Web de « moyen » à « haut ». L'utilisateur est averti lorsqu'une *applet* non signé est chargé dans le navigateur. Cela permet d'empêcher l'exécution automatique et silencieuse d'une *applet* Java sur le poste client. Cette fonctionnalité est aussi appelée « Click2Play ».

Le 20 janvier 2013, un chercheur a affirmé que Java 7 mise à jour 11 était toujours vulnérable. Il n'y a pas de code d'exploitation public et le chercheur a envoyé sa preuve de concept à Oracle pour corriger la vulnérabilité. Un autre chercheur a montré qu'il était possible de contourner la protection « Click2Play » dans la mise à jour 11 de Java. Le contournement consiste à sérialiser son *applet* Java et à utiliser la balise `object` à la place de la balise `code` dans la page Web de l'*applet*.

Le 1er février 2013, Oracle a publié la version 7 mise à jour 13 de Java (cf. CERTA-2013-AVI-092). Il s'agit là encore d'une mise à jour « hors cycle » de Oracle qui corrige 39 vulnérabilités non spécifiées par l'éditeur. La première vulnérabilité du code d'exploitation du 10 janvier 2013 n'est toujours pas corrigée par Oracle. On constate par contre que des vérifications ont été rajoutées dans l'API `Reflection`. On peut supposer, sans

pouvoir le confirmer actuellement, que ces vérifications interviennent suite à la publication de la preuve de concept du 20 janvier 2013. Le contournement de la protection « Click2Play » a aussi été corrigé dans cette mise à jour.

Le CERTA recommande d'appliquer la mise à jour 13 le plus rapidement possible lorsque la désactivation de Java dans le navigateur n'est pas possible et de suivre les règles de base de sécurité qui sont :

- de prendre garde aux liens qui sont dans les courriels;
- de faire preuve de vigilance lorsque vous consultez des sites Web non vérifiés.

Documentation

- Bulletin de version Oracle
  http://www.oracle.com/technetwork/java/javase/7u13-relnotes-1902884.html

2 Publications involontaires d'éléments sensibles

Le site Internet de gestion de version GitHub a été obligé de désactiver sa fonction de recherche dans les projets de développement le 23 janvier 2013. En effet, des utilisateurs ont remarqué, suite à l'amélioration du moteur de recherche, qu'il était possible de récupérer de nombreuses informations sensibles déposées par des développeurs : clés privées SSH, historiques de commandes comprenants des mots de passe, fichiers de configurations, etc. Ces informations avaient été déposées par mégarde, généralement lors de l'envoi de dossiers complets.

GitHub a depuis modifié sa fonction de recherche pour ne plus montrer ce type de fichiers.

Cet incident montre qu'il est nécessaire d'avoir la plus grande prudence lors de copie de fichiers sur un système tiers, local ou non. Certains de ces fichiers peuvent contenir des informations qui doivent rester confidentielles pour des questions de sécurité. Il est ainsi important de bien évaluer la confidentialité de chaque fichier copié et de préter une attention particulière aux fichiers qui ne sont pas directement visibles, mais néanmoins transférés, comme ce fut le cas pour les clés privées SSH copiées sur GitHub. Une bonne pratique est de créer un nouveau dossier spécialement pour le transfert de l'information et d'évaluer la criticité de chaque fichier destiné à être copié.

Cette recommandation vaut pour tout stockage dans un espace accessible publiquement, y compris de manière indirecte. Par exemple, il convient de faire particulièrement attention aux répertoires exposés par le Web, même si ceux-ci sont théoriquement invisibles.

Le CERTA recommande donc d'utiliser la copie de fichiers sur un système public en appliquant ces bonnes pratiques afin de s'assurer que seules les informations publiques souhaitées sont publiées.

3 Le schéma français de certification

La protection des systèmes d'information de l'Etat et des opérateurs d'importance vitale nécessite l'utilisation de technologies dont la sécurité est éprouvée. Le *référentiel général de sécurité* (RGS) fixe les règles et les mesures à mettre en place par les administrations en matière de sécurité des systèmes d'information, et impose notamment l'utilisation de produits qualifiés ou, à défaut, conformes au RGS. Il s'appuie pour cela sur le schéma français d'évaluation et de certification, dont la gestion est confiée à l'ANSSI. La liste publique des produits certifiés et des produits qualifiés est consultable sur le site internet de l'ANSSI.

Fonctionnement du schéma français d'évaluation et de certification

Le décret 2002-535 du 18 avril 2002 modifié fixe les règles de fonctionnement de ce schéma.

L'évaluation est menée par un laboratoire agréé par l'ANSSI (CESTI, Centre d'Évaluation de la Sécurité des Technologies de l'Information) sur la base de ses compétences en matière d'analyse technique de la sécurité. Les évaluations sont conduites selon des critères et une méthodologie qui assurent un certain niveau de confiance dans les travaux réalisés en rendant ceux-ci répétables et reproductibles. Actuellement, deux types de critères sont utilisés en France :

- les Critères Communs (CC) : il s'agit d'un standard internationalement reconnu s'inscrivant dans des accords de reconnaissance multilatéraux. Afin d'ajuster le coût de l'évaluation au besoin de sécurité, les CC proposent plusieurs niveaux de confiance. Plus le niveau visé est élevé, plus les contraintes en termes d'éléments de preuve que doit fournir le développeur au laboratoire sont importantes et plus les coûts d'évaluation sont élevés. Une évaluation CC dure en moyenne entre 6 et 18 mois (selon le type de produit, le niveau visé et la maturité du développeur) et nécessite des moyens financiers importants.

– la certification de sécurité de premier niveau (CSPN) : elle a été mise en place par l'ANSSI en 2008 pour proposer une alternative aux évaluations CC, dont le coût et la durée peuvent être un obstacle, lorsque le niveau de confiance visé est moins élevé. L'évaluation CSPN consiste en des tests en « boîte noire » effectués en temps (2 mois) et charge (25 ou 35 hommes x jours) contraints. La CSPN est une sorte de tamis permettant de discriminer à moindre coût les produits offrant un niveau de sécurité satisfaisant des autres. Malgré la charge réduite, environ 50% des produits échouent dans cette évaluation.

La certification est la validation par une tierce partie (l'ANSSI) que l'évaluation s'est déroulée dans les règles de l'art et en toute impartialité. Elle confirme que le produit répond bien aux exigences listées dans sa cible de sécurité et donne lieu à un rapport de certification ainsi qu'à un certificat. Ceux-ci peuvent être reconnus à l'international en vertu des accords signés par l'ANSSI.

Activité du schéma national d'évaluation et de certification

Aujourd'hui l'ANSSI délivre près d'une centaine de certificats par an (90% de certificats CC et 10% de certificats CSPN) ce qui en fait un des premiers émetteurs mondiaux. Les utilisateurs du schéma sont des industriels ou des prescripteurs en matière de sécurité, comme le GIE-CB pour les cartes bancaires, le GIE-SESAM Vitale pour les cartes vitales ou encore l'ANTS (Agence Nationale des Titres Sécurisés) pour les passeports électroniques. Le schéma de certification développe continuellement de nouvelles méthodologies et de nouveaux services pour répondre au mieux aux besoins des utilisateurs et pour s'adapter aux évolutions technologiques.

La qualification

La *qualification* est un label de l'ANSSI qui s'inscrit dans le Référentiel Général de Sécurité (RGS) pour les produits de sécurité destinés à être utilisés par l'administration. La qualification s'appuie sur le processus de certification auquel sont ajoutés quelques compléments comme la validation de la cible de sécurité par l'ANSSI comme répondant aux besoins de l'administration, l'obligation de conformité au référentiel cryptographique de l'ANSSI, etc. Trois niveaux de qualification sont définis, correspondant à trois niveaux d'évaluation donc trois niveaux de confiance différents.

Documentation

– Liste des produits certifiés critères communs
http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cc/
– Liste des produits certifiés CSPN
http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/
– Liste des CESTI agréés critères communs
http://www.ssi.gouv.fr/fr/certification-qualification/cesti/les-cesti-agrees-pour-les-evaluations-cc-et-itsec.html
– Liste des CESTI agréés CSPN
http://www.ssi.gouv.fr/fr/certification-qualification/cesti/centres-d-evaluation-agrees-pour-la-cspn.html
– Décret numéro 2002-535 du 18 avril 2002 modifié
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412673&dateTexte=20130208

4 Rappel des avis émis

Dans la période du 01 février au 08 février 2013, le CERTA a émis les publications suivantes :
– CERTA-2013-AVI-084 : Vulnérabilité dans IBM Sterling Connect:Direct
– CERTA-2013-AVI-085 : Multiples vulnérabilités dans Wireshark
– CERTA-2013-AVI-086 : Multiples vulnérabilités dans MariaDB
– CERTA-2013-AVI-087 : Multiples vulnérabilités dans Novell GroupWise
– CERTA-2013-AVI-088 : Multiples vulnérabilités dans VMware vSphere
– CERTA-2013-AVI-089 : Vulnérabilité dans HP Network Node Manager i
– CERTA-2013-AVI-090 : Multiples vulnérabilités dans IBM InfoSphere Balanced Warehouse
– CERTA-2013-AVI-091 : Multiples vulnérabilités dans Apple MacOS X
– CERTA-2013-AVI-092 : Multiples vulnérabilités dans Oracle Java

- CERTA-2013-AVI-093 : Multiples vulnérabilités dans EMC RSA Archer
- CERTA-2013-AVI-094 : Multiples vulnérabilités dans IBM WebSphere
- CERTA-2013-AVI-095 : Multiples vulnérabilités dans IBM Tivoli Storage Manager
- CERTA-2013-AVI-096 : Multiples vulnérabilités dans JBoss Enterprise Application Platform
- CERTA-2013-AVI-097 : Multiples vulnérabilités dans Apple OS X Server
- CERTA-2013-AVI-098 : Multiples vulnérabilités dans Xen
- CERTA-2013-AVI-099 : Multiples vulnérabilités dans OpenSSL
- CERTA-2013-AVI-100 : Vulnérabilité dans Cisco ATA 187
- CERTA-2013-AVI-101 : Vulnérabilité dans IBM Storwize V7000
- CERTA-2013-AVI-102 : Vulnérabilité dans Cisco NX-OS

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2012-ALE-001-001 : Vulnérabilité dans Cisco IronPort (fermeture de l'alerte, suite à la correction par l'éditeur)

Gestion détaillée du document

08 février 2013 version initiale.