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 26 octobre 2015
N° CERTFR-2015-ACT-043

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-043

1 - Bulletin de sécurité Oracle

Lors de la publication de son bulletin de sécurité principal du 20 octobre 2015, Oracle a annoncé la correction de 154 vulnérabilités concernant 57 de ses produits, notamment :

- Oracle Database Server
- Oracle MySQL
- Oracle Java SE
- Oracle Sun Systems
- Oracle Solaris
- Oracle Linux
- Oracle VM Virtualbox

Les vulnérabilités touchant Oracle Database Server sont considérées par l'éditeur comme moyennes ou importantes. 7 vulnérabilités sont corrigées par cette mise à jour.

La vulnérabilité CVE-2015-4863 sur le composant Portable Clusterware est considérée comme très critique. Celle-ci permet à un attaquant d'effectuer une attaque à distance sans authentification préalable. Oracle n'indique pas le type de vulnérabilités susceptibles d'être exploitées par l'attaquant et l'origine de leur découverte dans la nature dans ses bulletins de sécurité.

Les vulnérabilités touchant Oracle MySQL sont considérées majoritairement par l'éditeur comme mineures ou importantes. 30 vulnérabilités sont couvertes par ce correctif, dont deux pouvant être exploitables à distance par un attaquant sans authentification préalable. La vulnérabilité CVE-2015-3144 dans le produit MySQL Enterprise Monitor est considérée comme critique.

Les vulnérabilités touchant Oracle Java SE sont considérées majoritairement par l'éditeur comme importantes ou critiques. La mise à jour corrige 25 vulnérabilités, dont 24 pouvant être exploitables à distance par un attaquant sans authentification préalable. Les vulnérabilités critiques affectent les composants Java SE et Java SE Embedded. Parmi celles-ci, les vulnérabilités très critiques (ayant un score de criticité de 10/10) sont au nombre de 7. La vulnérabilité CVE-2015-4902, à l'indice de criticité de 5, a été exploitée activement dans la nature conjointement avec la CVE-2015-2590 (corrigée en juillet) dans le cadre d'attaques ciblées.

Les vulnérabilités touchant les produits Oracle Sun Systems sont considérées majoritairement par l'éditeur comme allant de mineures à importantes. 29 vulnérabilités sont couvertes par ce correctif, dont 10 pouvant être exploitables à distance par un attaquant sans authentification préalable.

La vulnérabilité CVE-2013-4784 affectant les produits Fujitsu M10-1, M10-4 et M10-4S Servers est considérée comme très critique. Oracle indique dans ce bulletin la fin du support étendu pour Solaris 8 et Solaris 9. Ceux-ci ne bénéficieront plus désormais de correctifs de sécurité. Les vulnérabilités touchant les produits tiers intégrés à Oracle Solaris sont au nombre de trois. Toutes sont exploitables à distance par un attaquant sans authentification préalable.

Les vulnérabilités touchant Oracle Linux sont considérées majoritairement par l'éditeur comme moyennes ou importantes. 27 vulnérabilités sont corrigées, dont 17 pouvant être exploitables à distance par un attaquant sans authentification préalable. Ce bulletin ne comprend pas de vulnérabilités critiques.

Les vulnérabilités touchant les produits de virtualisation Oracle, dont Oracle VM Virtualbox, sont considérées majoritairement par l'éditeur comme mineures ou importantes. 11 vulnérabilités sont corrigées, dont 4 pouvant être exploitables à distance par un attaquant sans authentification préalable. Ce bulletin ne comprend pas de vulnérabilités critiques.

Le CERT-FR rappelle l'importance de l'application des correctifs de sécurité au vu de la criticité de certaines vulnérabilités et de l'exploitation de l'une d'entre elles dans la nature depuis juillet.

Documentation

- Bulletin de sécurité Oracle du 20 octobre 2015 :
  http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
- Bulletin de sécurité Oracle Linux du 20 octobre 2015 :
  http://www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
- Bulletin de sécurité Oracle Solaris du 20 octobre 2015 :
  http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
- CERTFR-2015-AVI-437 : Multiples vulnérabilités dans Oracle Database Server :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-437/index.html
- CERTFR-2015-AVI-438 : Multiples vulnérabilités dans Oracle MySQL :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-438/index.html
- CERTFR-2015-AVI-439 : Multiples vulnérabilités dans Oracle Java SE :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-439/index.html
- CERTFR-2015-AVI-440 : Multiples vulnérabilités dans Oracle Sun Systems :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-440/index.html
- CERTFR-2015-AVI-441 : Multiples vulnérabilités dans Oracle Solaris :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-441/index.html
- CERTFR-2015-AVI-442 : Multiples vulnérabilités dans Oracle Linux :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-442/index.html
- CERTFR-2015-AVI-443 : Multiples vulnérabilités dans Oracle VM Virtualbox :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-443/index.html
- CERTFR-2015-AVI-444 : Multiples vulnérabilités dans Oracle Peoplesoft :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-444/index.html
- CERTFR-2015-ALE-007 : Vulnérabilité dans Oracle Java SE :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-007/index.html

2 - Nouvelle vague de rançongiciels

Depuis la mi-octobre 2015, le CERT-FR constate une nouvelle vague de compromissions de type rançongiciel. Un rançongiciel est un programme malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles depuis le compte utilisateur dont la session est compromise. Celui-ci est exécuté soit par une action de l'utilisateur, soit en exploitant une vulnérabilité du système. À travers une boîte de dialogue, la victime est ensuite invitée à verser de l'argent afin que l'attaquant déchiffre les fichiers ciblés. La somme généralement exigée dans le cadre de cette campagne est de quatre bitcoins(environ mille euros). L'adresse de courriel helpme@freespeechmail.org._BAD_ est également mentionnée dans l'extension chiffrée des documents.

Aujourd'hui, le CERT-FR n'a pas connaissance de moyens fiables pour récupérer la clé de chiffrement utilisée par le code malveillant.

Le CERT-FR tient à souligner que le recouvrement des données après paiement n'est en aucun cas garanti. Au-delà de l'incitation à réaliser ce type d'attaques, le recours à un moyen de paiement par carte bleue et la transmission des documents chiffrés à l'attaquant pour déchiffrement exposent la victime à des utilisations frauduleuses de ceux-ci.

Mesures préventives

Le CERT-FR recommande de sensibiliser les utilisateurs aux risques associés aux messages électroniques pour éviter l'ouverture de pièces jointes. Il convient en effet de ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes. Les utilisateurs ne doivent pas ouvrir des messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse. Plus généralement, il convient de mettre à jour les postes utilisateurs, notamment le système d'exploitation et les applications exposées sur Internet (lecteur PDF, lecteur messagerie, navigateurs et greffons) dans le cas où le code malveillant (ou une variante) exploiterait une vulnérabilité logicielle. Le CERT-FR recommande de configurer sur les postes de travail les restrictions logicielles pour empêcher l'exécution de code à partir d'une liste noire de répertoires :

- Si la solution utilisée est AppLocker, les règles de blocage suivantes doivent être définies :
  - OSDRIVE\Users*\AppData\
  - OSDRIVE\Windows\Temp\
- Si les restrictions logicielles (SRP) sont utilisées, les règles de blocage suivantes doivent être définies :
  - UserProfile\AppData
  - SystemRoot\Temp

Il est important de vérifier que le service "Application Identity" (AppIDSvc) est paramétré en démarrage automatique sur l'ensemble des postes pour que les restrictions logicielles soient opérantes (ce mode de démarrage peut être paramétré à travers une politique de groupe sur le domaine Windows). Si des dysfonctionnements sont rencontrés suite au déploiement de ces règles de blocage, il est nécessaire d'identifier les applications légitimes situées dans ces répertoires, et de définir des règles en liste blanche afin d'autoriser leur exécution.

Le CERT-FR recommande également de mettre à jour les logiciels antivirus du parc informatique (postes utilisateurs, passerelle de messagerie, etc.). Le code malveillant étant polymorphe, les éditeurs antivirus ont besoin de publier des signatures en constante évolution. Par ailleurs, il convient d'envoyer dès que possible un exemplaire du code malveillant à votre éditeur de logiciel antivirus si la variante n'est pas détectée par ce dernier.

Enfin, le CERT-FR recommande d'effectuer des sauvegardes saines et régulières des systèmes et des données (postes de travail, serveurs) puis de vérifier qu'elles se sont correctement déroulées. Les sauvegardes antérieures ne doivent pas être écrasées (cas où une version chiffrée aurait été sauvegardée). Les sauvegardes doivent être réalisées en priorité sur les serveurs hébergeant des données critiques pour le fonctionnement de l'entité. Celles-ci doivent être stockées sur des supports de données isolés du réseau en production.

Mesures réactives

Si le code malveillant est découvert sur vos systèmes, le CERT-FR recommande de déconnecter immédiatement du réseau les machines identifiées comme compromises. L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés. Le CERT-FR recommande aussi d'alerter le responsable sécurité ou le service informatique au plus tôt. Le temps de revenir à une situation normale, le CERT-FR recommande également de positionner les permissions des dossiers partagés en LECTURE SEULE afin d'empêcher la destruction des fichiers sur les partages. Les personnels pourront continuer de travailler localement et mettre à jour ultérieurement le partage. Aussi, le CERT-FR recommande de prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.

Le CERT-FR recommande également de bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant. L'objectif est de prévenir toute nouvelle compromission sur le même site. En complément, le CERT-FR recommande de rechercher et supprimer les messages malveillants similaires dans les boîtes de messagerie des utilisateurs. Par ailleurs, le CERT-FR recommande la réinstallation complète du poste et la restauration d'une sauvegarde réputée saine des données de l'utilisateur. De plus, dans le cadre de l'utilisation de profils itinérants, il convient de supprimer la copie serveur du profil afin de prévenir la propagation des codes malveillants par ce biais.

Enfin, les fichiers chiffrés peuvent être conservés par la victime au cas où dans le futur, un moyen de recouvrement des données originales serait découvert.

3 - Rappel des avis émis

Dans la période du 19 au 25 octobre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-ALE-012 : Campagne de messages électroniques non sollicités de type Dridex
- CERTFR-2015-AVI-433 : Multiples vulnérabilités dans PostgreSQL
- CERTFR-2015-AVI-434 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-435 : Multiples vulnérabilités dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-436 : Multiples vulnérabilités dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-437 : Multiples vulnérabilités dans Oracle Database Server
- CERTFR-2015-AVI-438 : Multiples vulnérabilités dans Oracle MySQL
- CERTFR-2015-AVI-439 : Multiples vulnérabilités dans Oracle Java SE
- CERTFR-2015-AVI-440 : Multiples vulnérabilités dans Oracle Sun Systems
- CERTFR-2015-AVI-441 : Multiples vulnérabilités dans Oracle Solaris
- CERTFR-2015-AVI-442 : Multiples vulnérabilités dans Oracle Linux
- CERTFR-2015-AVI-443 : Multiples vulnérabilités dans Oracle VM Virtualbox
- CERTFR-2015-AVI-444 : Multiples vulnérabilités dans Oracle Peoplesoft
- CERTFR-2015-AVI-445 : Multiples vulnérabilités dans Cisco ASA Software
- CERTFR-2015-AVI-446 : Vulnérabilité dans Drupal
- CERTFR-2015-AVI-447 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2015-AVI-448 : Multiples vulnérabilités dans le lecteur Flash intégré à Google Chrome
- CERTFR-2015-AVI-449 : Multiples vulnérabilités dans NTP
- CERTFR-2015-AVI-450 : Vulnérabilité dans phpMyAdmin

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

- CERTFR-2015-ALE-011 : Vulnérabilité dans Adobe Flash Player (clotûre de l'alerte)

Gestion détaillée du document

26 octobre 2015 version initiale.