Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 octobre 2013
N° CERTA-2013-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-042

1 - Porte dérobée dans les routeurs D-Link

Depuis le 12 octobre 2013 de nombreux sites Internet se font écho de la découverte d'un chercheur ayant analysé la partie du *firmware* de routeurs *D-Link* responsable de l'authentification. Cette analyse a révélé la présence d'une porte dérobée permettant un accès direct à l'interface d'administration de l'équipement, en contournant complètement le mécanisme d'authentification.

Les informations techniques ainsi que des codes permettant l'exploitation de cette faille de sécurité ayant été diffusés publiquement, le risque de compromission des équipements vulnérables exposant leur interface d'administration sur Internet est très important. Il est d'autant plus grand que l'identification de ces équipements est facilitée par l'existence de moteur de recherches spécifiques, comme *shodan*, qui donne aux attaquants le moyen d'établir très rapidement une liste de cibles potentielles.

Le type de routeurs affectés ciblant plus principalement le grand public que le milieu professionnel, le CERTA n'a pas levé d'alerte. Cependant, dans l'hypothèse où des équipements vulnérables seraient identifiés, le CERTA recommande de vérifier que leur interface d'administration est accessible uniquement depuis des postes légitimes et de s'assurer que celle-ci n'est pas publiquement exposée sur Internet (cf. Règle 25 du Guide d'Hygiène Informatique). De plus, et particulièrement dans le cas où l'interface était exposée, le CERTA insiste sur la nécessité de consulter les journaux de l'équipement et des équipements adjacents, afin de déterminer si des connexions illégitimes ont été effectuées sur le routeur. Il est également fortement recommandé de suivre la publication de correctifs sur le site de *D-Link* et d'appliquer ces derniers dès que possible. Dans l'intervalle, le CERTA conseille de faire preuve d'une vigilance accrue concernant les actions d'administrations effectuées sur ces équipements via la consultation régulière des journaux. D'après le constructeur, les mises à jour des *firmwares* corrigeant la vulnérabilité devraient être disponibles d'ici la fin du mois.

Documentation

- Guide d'hygiène informatique de l'ANSSI :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Site du support D-Link :
  http://www.dlink.com/uk/en/support/security

2 - Vulnérabilité suite à l'installation de systèmes de gestion de contenu (SGC)

La plupart des SGC proposent un assistant d'installation qui consiste en une suite de pages Web permettant de configurer l'application. Lors de la création de l'arborescence du SGC à son installation, cet assistant est généralement copié dans un répertoire accessible à tout utilisateur, même non authentifié. À la fin de l'installation, il est très souvent indiqué de supprimer ce répertoire. Si cette opération n'est pas réalisée, une personne malveillante peut alors prendre le contrôle de l'application et reconfigurer le SGC.

Le CERTA a récemment pu constater des cas d'exploitations malveillantes de cette erreur de configuration et recommande par conséquent de suivre les procédures d'installation jusqu'à leur terme. Pour tous les SGC déjà installés, il est également recommandé de vérifier que le répertoire d'installation a bien été supprimé.

3 - Microsoft Windows et Address Space Layout Randomization

La protection ASLR (Address Space Layout Randomization) est incluse par défaut dans les produits Windows depuis l'arrivée de Microsoft Vista en Janvier 2007. L'ASLR permet de placer de façon aléatoire les zones de données dans la mémoire virtuelle du processus. Cette protection permet de limiter le fonctionnement des attaques se basant sur des adresses fixes comme par exemple le ROP (Return-Oriented Programming).

Le CERTA rencontre une recrudescence des codes d'exploitation utilisant des contournements de cette protection afin de fiabiliser son exploitation. Les contournements ont été utilisés dans des codes d'exploitation ciblant deux vulnérabilités d'Internet Explorer :

- CVE-2013-3893 (CERTA-2013-ALE-006)
- CVE-2012-4792 (CERTA-2012-ALE-010)

La technique la plus répandue (car la plus simple) pour contourner la protection ASLR est d'utiliser une bibliothèque qui est chargée dans une zone fixe du processus cible. Pour qu'une bibliothèque soit compatible avec la protection ASLR, il est nécessaire de la compiler avec l'option `/DYNAMICBASE` du compilateur de Visual Studio.

Par exemple, Microsoft Office 2010 et 2007 sont livrés avec la bibliothèque `HXDS.DLL` qui n'a pas été compilée avec l'option précédente. Le chargement de cette bibliothèque dans Internet Explorer est possible en ouvrant via une URL de type `ms-help://`. L'utilisation de ce contournement est donc limité aux machines sur lesquelles Microsoft Office 2010 ou 2007 seraient installés.

Java version 1.6 est aussi livré avec une bibliothèque (`MSVCR71.DLL`) qui n'a pas été compilée avec le support de l'ASLR. Cette bibliothèque est donc accessible par l'attaquant dans l'espace mémoire d'Internet Explorer. Cette attaque est donc possible sur les machines sur lesquelles Oracle Java 6 est installé.

Une possibilité de contournement supplémentaire a été corrigée par Microsoft avec la mise à jour MS13-063. Le bulletin d'actualité CERTA-2013-ACT-033 donne plus d'informations sur ce contournement qui consistait à utiliser une région fixe en mémoire(`ntdll!SharedUserData`) pour contourner la protection active de la mémoire du système.

Afin de se prémunir de l'utilisation de ces contournements dans un code d'exploitation, le CERTA recommande d'appliquer les correctifs de sécurité et d'utiliser la dernière version supportée de Microsoft Windows, Microsoft Office et de Oracle Java. Le CERTA rappelle que Java 6 n'est plus supporté par Oracle et qui convient de migrer au plus vite vers la dernière version supportée de ce produit.

Documentation

- Techniques de contournement d'ASLR :
  http://www.fireeye.com/blog/technical/cyber-exploits/2013/10/aslr-bypass-apocalypse-in-lately-zero-day-exploits.html
- Alerte CERTA-2012-ALE-010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-010/
- Alerte CERTA-2013-ALE-006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-006/

4 - Nouvelles fonctionnalités de sécurité dans Windows 8.1

Récemment, la société Microsoft a publié la version 8.1 de son système d'exploitation Windows qui apporte de nouvelles fonctionnalités de sécurité.

Parmi les grandes évolutions, se distinguent :

- Internet Explorer 11, dont la protection des greffons a été renforcée par le scan des données qui vont être exécutées ;
- l'implémentation de *Secure Boot* dans `UEFI`, afin de vérifier la chaîne de démarrage via des signatures numériques ;
- le chiffrement des périphériques externes par défaut ;

– la généralisation des applications pouvant tirer partie de la biométrie (l'accès à distance, l'UAC, l'authentification des sessions) et le support de lecteurs d'empreintes capables de détecter de fausses empreintes en silicone ;
– le chiffrement et le marquage des données d'entreprise, ainsi que la possibilité d'effacer certaines données en fonction de l'utilisateur ;
– l'inclusion d'un système de détection heuristique réseau (NIPS) dans Windows Defender pour lutter contre des menaces inconnues ;
– la possibilité de limiter l'accès au Windows Store via l'utilisation de profils prédéfinis en environnement professionnel.

Ces fonctionnalités ont été précédées par un ensemble d'améliorations portées par Microsoft depuis Windows 8 pour lutter contre l'exécution de code en mémoire (utilisation de l'ASLR pour la pile, le tas, le PEB/TEB, etc.), comme détaillé dans son dernier rapport sur les tendances d'exploitation logicielle.

De façon générale, le CERTA recommande de migrer autant que possible, vers les dernières versions des systèmes d'exploitation fournis par les éditeurs, afin de pouvoir bénéficier des nouvelles fonctionnalités de sécurité renforcées qu'elles apportent.

Documentation

– Bulletin technet des changements des technologies de sécurité pour Windows 8.1 :
http://technet.microsoft.com/en-us/library/dn344918.aspx
– Rapport sur les tendances d'exploitation logicielle :
http://www.microsoft.com/en-us/download/details.aspx?id=39680

5 - Correctifs Oracle

Dans le cadre de son cycle de diffusion des mises à jour, Oracle a publié son "Critical Patch Update" (CPU) d'octobre 2013. A noter que cet ensemble de correctifs intègre dorénavant les correctifs Java qui étaient jusqu'alors publiés séparément par Oracle.

Cette mise à jour corrige 127 vulnérabilités :
– 51 vulnérabilités pour *Oracle Java SE*, dont 50 sont exploitables à distance sans authentification ;
– 17 vulnérabilités pour *Oracle Fusion Middleware*, dont 12 sont exploitables à distance sans authentification ;
– 12 vulnérabilités pour la suite *Oracle and Sun Systems Products*, dont 5 sont exploitables à distance sans authentification ;
– 9 vulnérabilités pour *Oracle Siebel CRM*, dont 5 sont exploitables à distance sans authentification ;
– 8 vulnérabilités pour *Oracle PeopleSoft Products*, dont 5 sont exploitables à distance sans authentification ;
– 8 vulnérabilités pour *Oracle MySQL*, dont 1 qui affecte intégralement la confidentialité, l'intégrité et la disponibilité du système ;
– 6 vulnérabilités pour *Oracle Industry Applications* qui affectent l'intégrité, la confidentialité ainsi que la disponibilité du système ;
– 4 vulnérabilités pour *Oracle Enterprise Manager Grid Control*, toutes exploitables à distance sans authentification et qui affectent l'intégrité du système ;
– 2 vulnérabilités pour *Oracle Database server*, exploitables à distance sans authentification et qui affectent la confidentialité du système ;
– 2 vulnérabilités pour la suite *Oracle Supply Chain Products*, exploitables à distance sans authentification qui affectent l'intégrité et la disponibilité du système ;
– 2 vulnérabilités pour *Oracle iLearning*, exploitables à distance sans authentification affectant l'intégrité, la confidentialité et la disponibilité du système ;
– 2 vulnérabilités pour la suite *Oracle Primavera Products*, dont 1 est exploitable à distance sans authentification. Elles affectent la confidentialité et l'intégrité du système ;
– 2 vulnérabilités pour *Oracle Virtualization*, dont 1 est exploitable à distance sans authentification. Elles affectent la disponibilité du système ;
– 1 vulnérabilité pour la suite *Oracle E-Business*, exploitable à distance sans authentification et affectant la confidentialité du système ;
– 1 vulnérabilité pour *Oracle Financial Services Software*, qui affecte la confidentialité, l'intégrité ainsi que la disponibilité du système.

Le CERTA recommande d'appliquer ces mises à jour le plus rapidement possible.

Documentation

- Bulletin de sécurité Oracle JavaCPUoct2013 du 18 juin 2013 :
  http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.htmlAppendixJAVA
- Avis CERTA-2013-AVI-574 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-574/
- Avis CERTA-2013-AVI-575 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-575/
- Avis CERTA-2013-AVI-576 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-576/
- Avis CERTA-2013-AVI-577 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-577/
- Avis CERTA-2013-AVI-578 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-578/
- Avis CERTA-2013-AVI-579 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-579/
- Avis CERTA-2013-AVI-580 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-580/
- Avis CERTA-2013-AVI-581 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-581/
- Avis CERTA-2013-AVI-582 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-582/
- Avis CERTA-2013-AVI-583 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-583/
- Avis CERTA-2013-AVI-584 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-584/
- Avis CERTA-2013-AVI-585 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-585/
- Avis CERTA-2013-AVI-586 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-586/
- Avis CERTA-2013-AVI-587 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-587/
- Avis CERTA-2013-AVI-588 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-588/
- Avis CERTA-2013-AVI-589 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-589/
- Avis CERTA-2013-AVI-590 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-590/

6 - Rappel des avis émis

Dans la période du 11 au 17 octobre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-570 : Vulnérabilité dans Xen qemu
- CERTA-2013-AVI-571 : Multiples vulnérabilités dans Juniper Junos OS
- CERTA-2013-AVI-572 : Vulnérabilité dans Symantec Management Platform Agent
- CERTA-2013-AVI-573 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-574 : Multiples vulnérabilités dans Oracle Database
- CERTA-2013-AVI-575 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2013-AVI-576 : Multiples vulnérabilités dans Oracle Enterprise Manager Grid Control
- CERTA-2013-AVI-577 : Vulnérabilité dans Oracle E-Business Suite
- CERTA-2013-AVI-578 : Multiples vulnérabilités dans Oracle Supply Chain Products Suite
- CERTA-2013-AVI-579 : Multiples vulnérabilités dans Oracle PeopleSoft Enterprise
- CERTA-2013-AVI-580 : Multiples vulnérabilités dans Oracle Siebel
- CERTA-2013-AVI-581 : Multiples vulnérabilités dans Oracle iLearning

- CERTA-2013-AVI-582 : Multiples vulnérabilités dans Oracle Health Sciences InForm
- CERTA-2013-AVI-583 : Vulnérabilité dans Oracle Retail Invoice Matching
- CERTA-2013-AVI-584 : Vulnérabilité dans Oracle FLEXCUBE
- CERTA-2013-AVI-585 : Multiples vulnérabilités dans Oracle Primavera Products Suite
- CERTA-2013-AVI-586 : Multiples vulnérabilités dans Oracle Java SE
- CERTA-2013-AVI-587 : Multiples vulnérabilités dans Oracle et Sun Systems Products Suite
- CERTA-2013-AVI-588 : Multiples vulnérabilités dans Oracle Virtualization
- CERTA-2013-AVI-589 : Multiples vulnérabilités dans Oracle MySQL
- CERTA-2013-AVI-590 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-591 : Vulnérabilité dans Ruby on Rails
- CERTA-2013-AVI-592 : Multiples vulnérabilités dans Puppet

Gestion détaillée du document

18 octobre 2013 version initiale.