Concours externe Inria 2013

Arrêté du 15 avril 2013

Poste ROC05 – Pilote d'exploitation administrateur systèmes et réseaux (h/f)

Accès au corps des assistants ingénieurs

Epreuve du 27 juin 2013
Note sur 20 – Coefficient 3 – Durée 2 heures

****

La notation prendra en compte la qualité des réponses, mais aussi la rédaction, la présentation, le style et l'orthographe.

Veuillez respecter l'anonymat dans les réponses.

Ne pas omettre de noter votre numéro d'ordre sur les feuilles intercalaires.

1. Administration système Linux (7 points)

1.1. Montage à distance

Sur un serveur Linux, vous souhaitez permettre à des utilisateurs en s'authentifiant de monter de façon sécurisée un espace de partage disponible entre 7h et 19h. Quels sont les composants logiciels à utiliser ? Comment procèderiez -vous ?

1.2. Partage de fichiers

Quel problème pose l'export par NFS de répertoires utilisateurs vers un parc de machines Unix sur lesquelles les utilisateurs ont des droits root ?

Quelle(s) solution(s) proposez-vous pour éliminer ce problème ?

1.3. Performances

Quelles sont les commandes permettant de détecter et d'analyser une dégradation des performances sur des postes Linux ?

1.4. SSH

Vous disposez de trois machines : C, B et S.

Hypothèses de départ :

- S est dans une zone dite sécurisée non accessible depuis l'extérieur du réseau de l'institut.
- C est dans un réseau hébergé dans une université ayant accès à tout l'internet et qui ne fait pas partie du réseau de l'institut.
- B est la seule machine de l'institut à être accessible via SSH depuis l'internet.

Précisez les hypothèses éventuelles que vous êtes amené(e) à faire ? Enoncez toutes les commandes nécessaires sur chacune des machines pour rendre accessible, depuis C une application Web tournant sur S.

1.5. Permission d'accès aux fichiers

- Donnez le résultat de la commande suivante et expliquez le :

```
chmod 4755 /home/gaston/mdp
```

- Donnez le résultat de la commande suivante et expliquez le :

```
chmod g+s /home/gaston/www
```

- Quelle est l'utilité du Sticky Bit ? Illustrez vos propos par un exemple.

1.6. Partitionnement

Comment configure-t-on une zone de SWAP sous Linux et à quoi sert-elle ?

1.7. Haute disponibilité

Quels sont les mécanismes de haute disponibilité logiciels sous Linux? Illustrez vos propos par des exemples.

---

2. Administration et infrastructure (10 points)

Windows

2.1. GPO

Qu'est ce qu'une GPO ? Sur quoi l'applique-t-on ?

2.2. Contrôleur de domaine

Quels sont les différents rôles du contrôleur de domaine d'un Active Directory ?

Réseau

2.3. DHCP (réseau/ administration système)

A quoi sert DHCP ? Quels types d'information véhicule-t-il ?

2.4. Masque et sous réseau

Qu'est ce qu'une classe de réseaux privés ? Citez une plage d'adressage privé et proposez un découpage de cette dernière de telle façon à obtenir 4 sous-réseaux respectifs d'au moins 30, 50 et 200 machines. Donnez ces 4 sous réseaux.

Virtualisation

2.5. Hyperviseur

Quelles sont les différences entre un hyperviseur de type 1 et un hyperviseur de type 2 ?

Sécurité

2.6. Authentification et identité

Quelles sont les différences entre CAS, Shibboleth et Kerberos ?

2.7. Compromission d'une machine

Quelles actions devez-vous entreprendre si vous recevez un message du CERT Renater vous signalant qu'une des machines de votre parc est compromise ?

Plateformes expérimentales

2.8. Calcul haute performance

Sur un système de calcul haute performance, pouvez-vous décrire le rôle d'un ordonnanceur et en citer des exemples?

2.9. Grille de calcul

En tant qu'administrateur d'une grille ou d'un cluster de calcul haute performance, quels sont les composants logiciels que vous vous attendez « devoir mettre » à disposition des utilisateurs?

Termes usuels

2.10. Acronymes

Regroupez les termes usuels de l'informatique énoncés ci-dessous dans 5 rubriques maximum auxquelles vous donnerez un intitulé : SNMP, X509, PERL, SHA, NTFS, SSD, EXT3, VBS, NAS, AJAX, NFS, PKI, UDP, SATA, MD5, ARP, VPN, ISCSI.

---

3. Etude de cas (3 points)

Rédaction d'une note (3 points)

A partir de l'avis du CERT disponible en annexe, vous devez présenter à votre responsable une note de quelques lignes résumant les conséquences de cet avis dont vous venez de prendre connaissance et le plan d'action que vous proposez. Vous devrez préciser toutes les hypothèses que vous seriez amené(e) à faire.

En complément, vous rédigerez un message d'information en anglais à destination des utilisateurs qui sera publié sur le serveur d'information de votre service présentant les conséquences éventuelles de la mise en œuvre de votre plan d'action sur l'activité des utilisateurs.

Hypothèses de départ :

Vous avez en charge un parc d'une centaine de machines sur lesquelles vous mettez à disposition des applications de gestion de contrats de recherche « webisées » provenant de différents partenaires (Inria, Université, ...) dont vous ne maitrisez pas les évolutions technologiques. Afin d'assurer les conditions opérationnelles nécessaires et de répondre au cahier des charges techniques des partenaires, vous avez jusqu'à présent conserver une version précise de JRE (java 7 update 2 maximum) sur les postes que vous administrez.

Annexe

Alert (TA13-010A)

Oracle Java 7 Security Manager Bypass Vulnerability

Original release date: January 10, 2013 | Last revised: February 06, 2013

Systems Affected

Any system using Oracle Java 7 (1.7, 1.7.0) including

- Java Platform Standard Edition 7 (Java SE 7)
- Java SE Development Kit (JDK 7)
- Java SE Runtime Environment (JRE 7)
- OpenJDK 7 and 7u
- IcedTea 2.x (IcedTea7 2.x)

All versions of Java 7 through update 10 are affected. Web browsers using the Java 7 plug-in are at high risk.

Overview

A vulnerability in the way Java 7 restricts the permissions of Java applets could allow an attacker to execute arbitrary commands on a vulnerable system.

Description

A vulnerability in the Java Security Manager allows a Java applet to grant itself permission to execute arbitrary code. An attacker could use social engineering techniques to entice a user to visit a link to a website hosting a malicious Java applet. An attacker could also compromise a legitimate web site and upload a malicious Java applet (a "drive-by download" attack).

Any web browser using the Java 7 plug-in is affected. The Java Deployment Toolkit plug-in and Java Web Start can also be used as attack vectors.

Reports indicate this vulnerability is being actively exploited, and exploit code is publicly available.

Further technical details are available in Vulnerability Note VU#625617.

Impact

By convincing a user to load a malicious Java applet or Java Network Launching Protocol (JNLP) file, an attacker could execute arbitrary code on a vulnerable system with the privileges of the Java plug-in process.

Solution

Update Java

Oracle Security Alert CVE-2013-0422 states that Java 7 Update 11 (7u11) addresses this (CVE-2013-0422) and a different but equally severe vulnerability (CVE-2012-3174).

Java 7 Update 11 sets the default Java security settings to "High" so that users will be prompted before running unsigned or self-signed Java applets.

Disable Java in web browsers

This and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered. To defend against this and future Java vulnerabilities, consider disabling Java in web browsers until adequate updates are available. As with any software, unnecessary features should be disabled or removed as appropriate for your environment.

Starting with Java 7 Update 10, it is possible to disable Java content in web browsers through the Java control panel applet. From Setting the Security Level of the Java Client:

> For installations where the highest level of security is required, it is possible to entirely prevent *any* Java apps (signed or unsigned) from running in a browser by de-selecting Enable Java content in the browser in the Java Control Panel under the Security tab.

If you are unable to update to Java 7 Update 10 please see the solution section of Vulnerability Note VU#636312 for instructions on how to disable Java on a per-browser basis.Vulnerability Note VU#625617

References

- Vulnerability Note VU#625617
- Setting the Security Level of the Java Client
- The Security Manager
- How to disable the Java web plug-in in Safari
- How to turn off Java applets
- NoScript
- Securing Your Web Browser
- Vulnerability Note VU#636312
- Oracle Security Alert CVE-2013-0422
- Security Alert for CVE-2013-0422 Released
- JDK 7u11 Release Notes

Revisions

- January 10, 2013: Initial release
- January 14, 2013: Added fix information per Java 7u11 release
- January 15, 2013: Added OpenJDK and IcedTea to Systems Affected