

[ VULNIT ]

Vulnerability  
Identification Tool

# Rapport d'audit

01 mars 2012, 16:22:29 - UTC

Version de l'outil	4.5
Nombre de cibles scannés	5
Nombre de vulnérabilités identifiées	38

# Sommaire

Sommaire	2
Introduction	3
Méthodologie	3
Appréciation du risque	3
Priorisation de traitement des vulnérabilités	3
Rapport à la direction	4
Vulnérabilités par priorité	4
Vulnérabilités, par fonction et objet	5
Vulnérabilités de priorité critique, par fonction et objet	6
Nombre de correctifs manquants, par IP et objet	7
Rapport technique	8
Inventaire	8
Résumé	10
WORKGROUP\OWASPBWA (192.168.1.21)	13
WORKGROUP\ORA9I (192.168.1.36)	24
VULNITLAB\SQL2K (192.168.1.45)	28
VULNITLAB\SQL2K5 (192.168.1.54)	32
VULNITLAB\WINXP (192.168.1.84)	46
Annexes	50
Annexe A: Glossaire	50
Annexe B: Outils d'audit	51
Annexe C : Génération du rapport	51
Légal	53
Copyright	53



## Introduction

L'outil d'audit VulnIT permet d'identifier de potentielles failles de sécurité informatique et le risque qu'elles pourraient engendrer en cas d'exploitation par un attaquant malveillant.

La première partie du rapport offre une vision synthétique et managériale des vulnérabilités de sécurité découvertes. La seconde partie liste exhaustivement ces vulnérabilités en apportant une évaluation de leur risque potentiel et des indications pour vous guider dans leur compréhension et leur résolution. Enfin, vous trouverez en annexe l'ensemble des serveurs et services découverts ce qui vous permettra le cas échéant d'approfondir leur examen.

## Méthodologie

Ce rapport ne peut prétendre à être exhaustif et ne se substitue donc en aucun cas à l'analyse qu'un expert en test d'intrusion mènerait. De plus, l'exactitude des informations qu'il contient doit être validée auprès de l'administrateur du système ciblé par l'audit, ce afin d'écartier toute erreur d'identification (faux positif) de l'outil.

## Appréciation du risque

L'évaluation du risque inhérent à chaque vulnérabilité figurant dans ce rapport repose sur la méthodologie CVSS (Common Vulnerability Scoring System), et prend en compte deux facteurs :

- l'impact potentiel d'une attaque exploitant cette vulnérabilité, en termes de disponibilité de l'application, confidentialité et intégrité des informations,
- l'exploitabilité (c'est-à-dire la facilité d'exploitation) de la vulnérabilité, une vulnérabilité plus facile à exploiter augmentant le nombre d'attaquants potentiels et donc la probabilité d'occurrence d'une attaque.

Les notes CVSS (risque global, impact et exploitabilité) s'échelonnent entre 0 et 10.

Seules les vulnérabilités de risque élevé (supérieur à 7) sont remontées dans ce rapport et doivent donc toutes faire l'objet d'une grande attention.

## Priorisation de traitement des vulnérabilités

La priorité de traitement suggérée pour chaque vulnérabilité a trois niveaux : critique (risque égal à 10), majeur (risque compris entre 8 et 10) ou élevé (risque compris entre 7 et 8).

Pour apprécier le risque réel de chaque vulnérabilité, il faut pondérer l'impact potentiel par la valeur de l'actif, c'est-à-dire l'importance opérationnelle d'une application ou la criticité de l'information pouvant être compromise ; et l'exploitabilité par l'exposition intrinsèque de l'entreprise - certaines activités type financières motivant plus d'attaques que d'autres.

Enfin, ces risques peuvent être couverts par des contrôles préventifs, dissuasifs ou palliatifs.



## Rapport à la direction

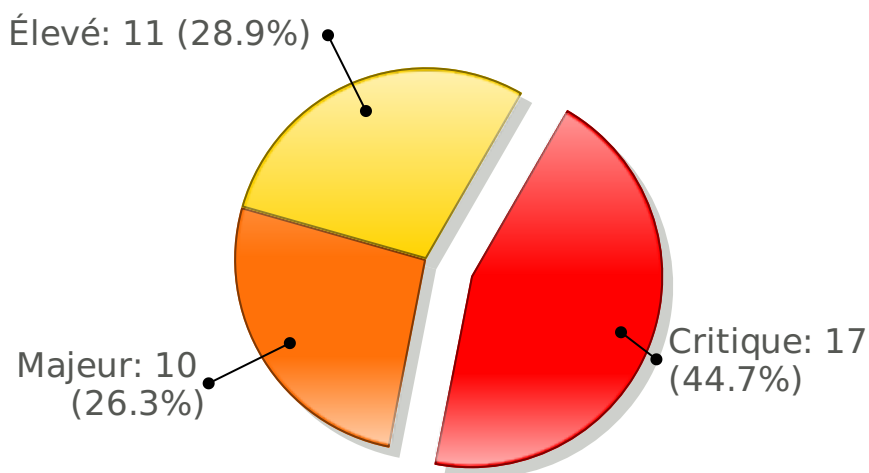
Résumé :

Parmi les 5 serveurs testés, 5 ont présenté des vulnérabilités dont **5 des vulnérabilité(s) de priorité critique**.

Ces vulnérabilités sont présentées graphiquement ci-dessous et détaillées dans la partie technique du rapport.

### Vulnérabilités par priorité

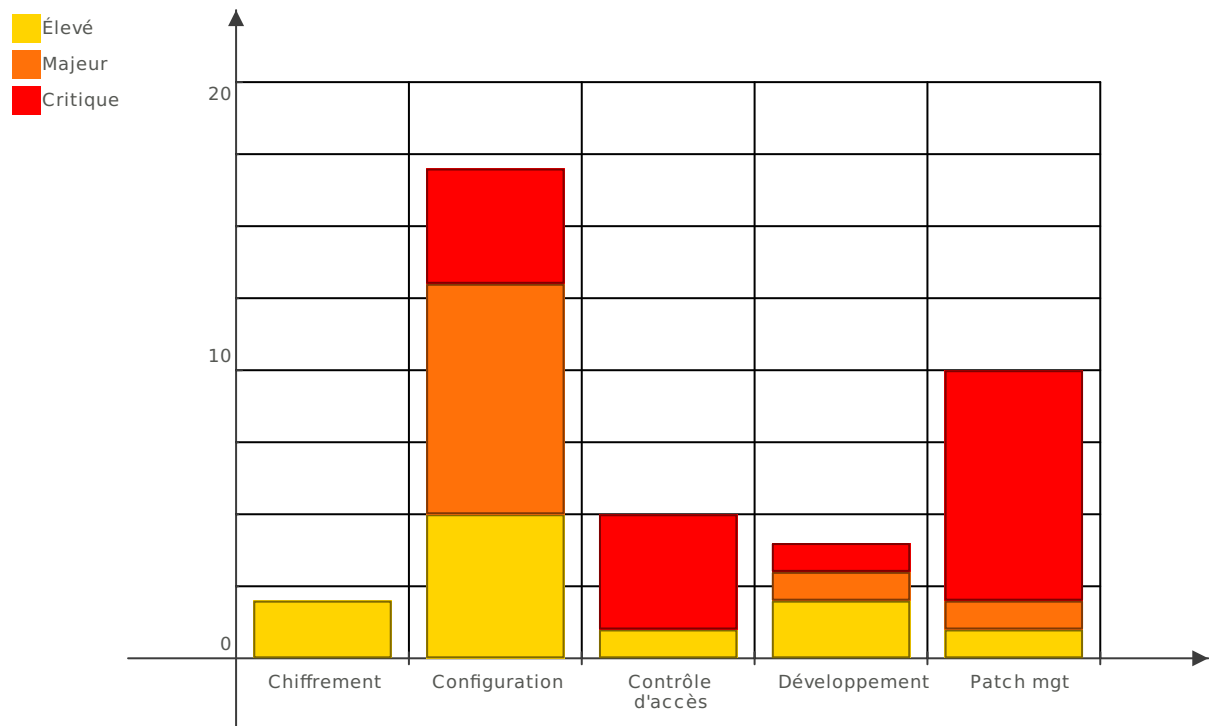
Ce graphique présente le nombre de vulnérabilités identifiées, par priorité.



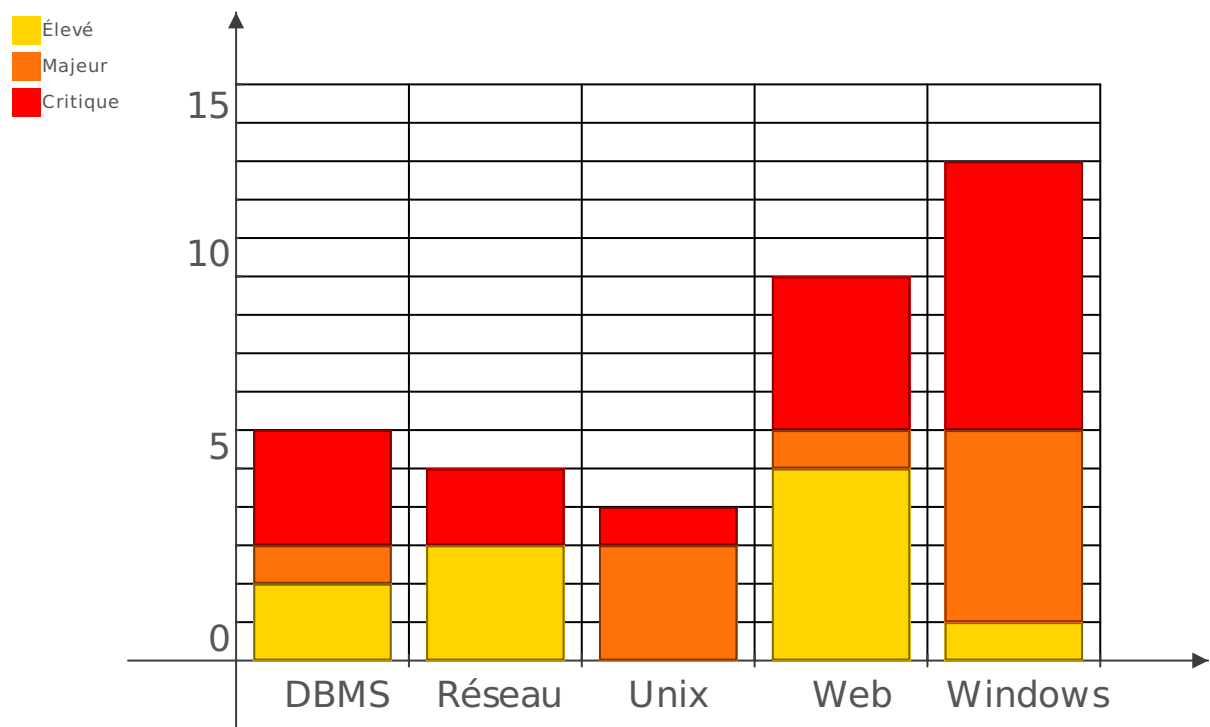


## Vulnérabilités, par fonction et objet

Ce graphique présente le nombre de vulnérabilités classées par fonction de contrôle.

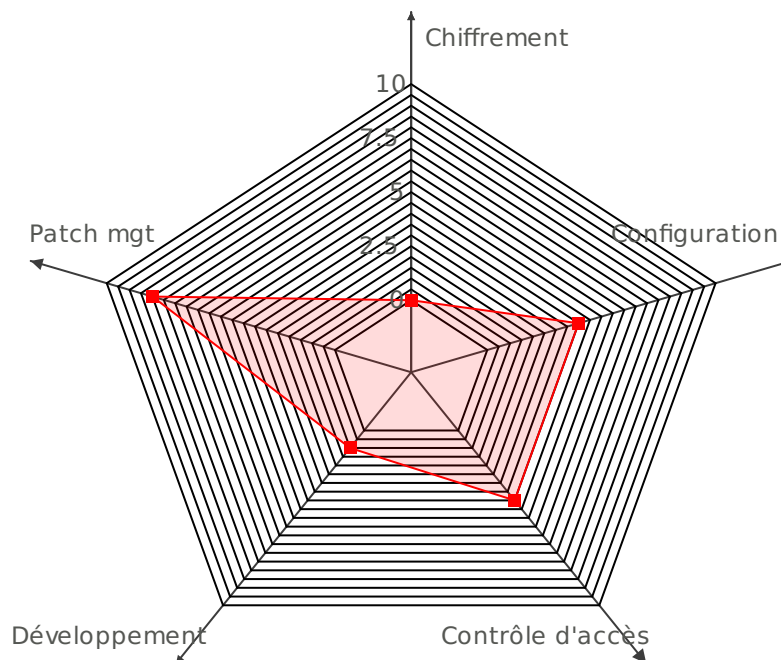


Ce graphique présente le nombre de vulnérabilités classées par objet de contrôle.

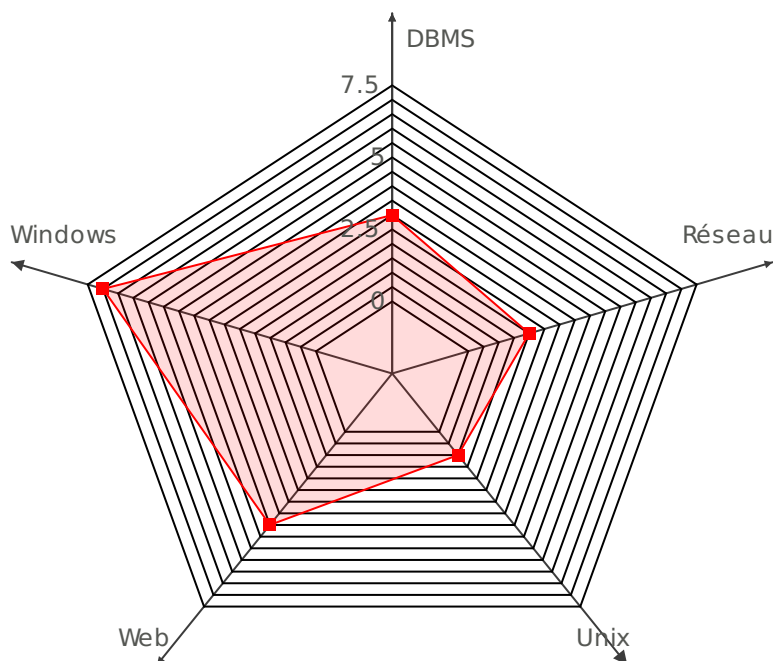


## Vulnérabilités de priorité critique, par fonction et objet

Ce graphique présente le nombre de vulnérabilités de priorité critique classées par fonction de contrôle.



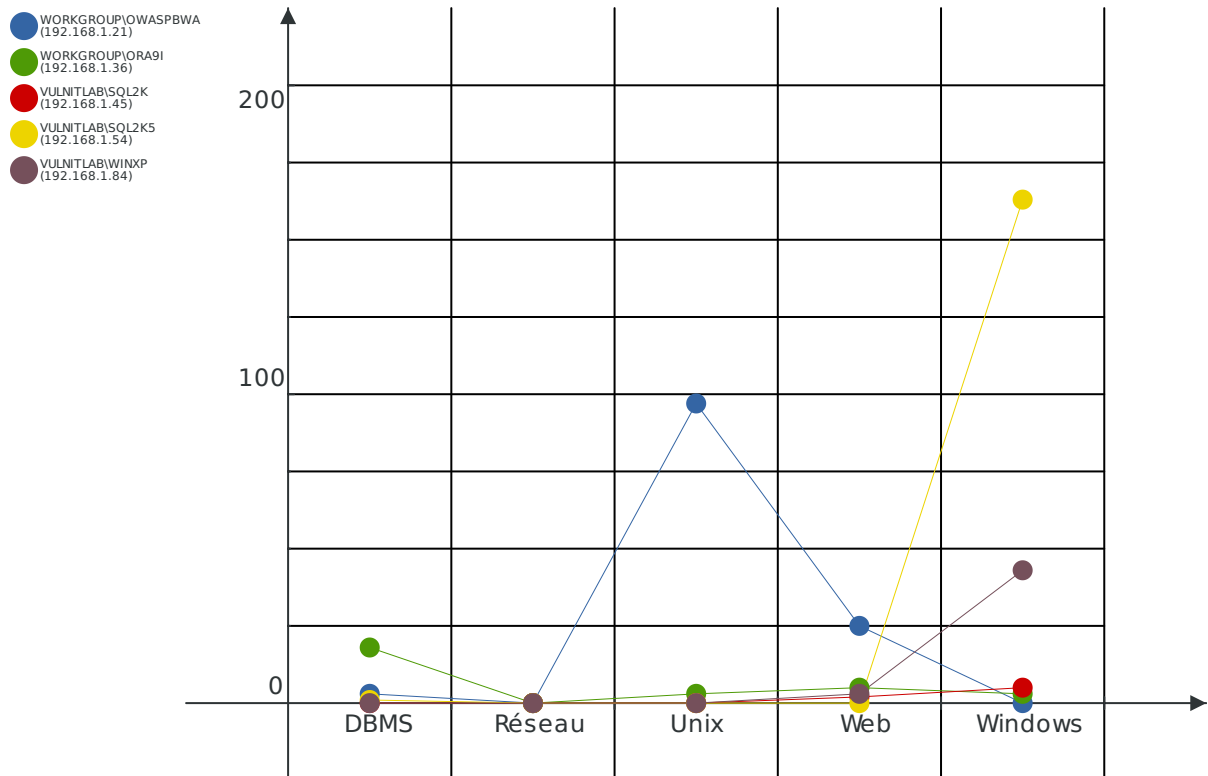
Ce graphique présente le nombre de vulnérabilités de priorité critique classées par objet de contrôle.





## Nombre de correctifs manquants, par IP et objet

Ce graphique présente le nombre de correctifs (*patches*) manquants pour chaque cible, classés par objet de contrôle.





# Rapport technique

## Inventaire

### **VULNITLAB\SQL2K (192.168.1.45)**

Date de dernier scan : 2012-02-22 17:49:02

Compte administrateur validé : non

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 7
- Majeur : 0
- Élevé : 2
- Ports ouverts : 27

Informations sur la machine distante :

- DNS : sql2k
- NetBios : VULNITLAB\SQL2K

Services :

- 7/tcp : echo - non testé
- 7/udp : echo - non testé
- 9/tcp : discard server
- 13/udp : daytime - non testé
- 13/tcp : daytime - non testé
- 17/tcp : Quote of the Day - non testé
- 19/tcp : ttytst source Character Generator - non testé
- 25/tcp : SMTP - Simple Mail Transfer Protocol
- 42/tcp : WINS - Windows Internet Naming Service - non testé
- 53/tcp : DNS - Domain Name Server
- 80/tcp : HTTP - World Wide Web - non testé
- 135/udp : RPC - Microsoft EPMAP - non testé
- 135/tcp : RPC - Microsoft EPMAP - non testé
- 137/udp : Netbios name service - non testé
- 139/tcp : NETBIOS Services
- 161/udp : SNMP
- 443/tcp : HTTPS - Secure HTTP
- 445/tcp : SMB - Microsoft File Sharing
- 515/tcp : Spooler - LPD
- 548/tcp : AFP - Apple Filing Protocol - non testé
- 1029/tcp : ms-lsa - non testé
- 1033/tcp : netinfo-local - non testé
- 1036/tcp : pcg-radar - non testé
- 1042/tcp : blah11 - non testé
- 1433/tcp : MSSQL - Microsoft SQL Server
- 1434/udp : MSSQL - Microsoft SQL Monitor - non testé
- 3372/tcp : MDTC - Microsoft Distributed Transaction Coordinator - non testé

### **WORKGROUP\OWASPBWA (192.168.1.21)**

Date de dernier scan : 2012-03-01 15:50:03

Compte administrateur validé : oui

Cible testée : oui

**Nombre de vulnérabilités :**

- Critique : 4
- Majeur : 4
- Élevé : 5
- Ports ouverts : 6

**Informations sur la machine distante :**

- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5
- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod\_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod\_python/3.3.1 Python/2.6.5 mod\_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5
- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod\_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod\_python/3.3.1 Python/2.6.5 mod\_perl/2.0.4 Perl/v5.10.1
- HTTPSERVER : Apache-Coyote/1.1
- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod\_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod\_python/3.3.1 Python/2.6.5 mod\_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5
- DNS : Inconnu(e)
- NetBios : WORKGROUP\OWASPBWA

**Services :**

- 22/tcp : SSH - Secure Shell Login
- 80/tcp : HTTP - World Wide Web - non testé
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing
- 5001/tcp : complex-link - non testé
- 8080/tcp : HTTP Alternate - non testé

**WORKGROUP\ORA9I (192.168.1.36)**

Date de dernier scan : 2012-02-29 16:57:02

Compte administrateur validé : non

Cible testée : oui

**Nombre de vulnérabilités :**

- Critique : 4
- Majeur : 0
- Élevé : 3
- Ports ouverts : 13

**Informations sur la machine distante :**

- DNS : ora9i
- NetBios : WORKGROUP\ORA9I

**Services :**

- 80/tcp : HTTP - World Wide Web - non testé
- 135/tcp : RPC - Microsoft EPMAP - non testé
- 137/udp : Netbios name service - non testé
- 139/tcp : NETBIOS Services
- 443/tcp : HTTPS - Secure HTTP
- 445/tcp : SMB - Microsoft File Sharing
- 1029/tcp : ms-lsa - non testé
- 1034/tcp : ActiveSync Notifications - non testé
- 1521/tcp : Oracle
- 1808/tcp : oracle-vp2 - non testé
- 2030/tcp : device2 - non testé
- 2100/tcp : FTP - File Transfer Protocol



- 8080/tcp : HTTP - World Wide Web - non testé

### **VULNITLAB\WINXP (192.168.1.84)**

Date de dernier scan : 2012-03-01 15:37:02

Compte administrateur validé : oui

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 1
- Majeur : 5
- Élevé : 0
- Ports ouverts : 3

Informations sur la machine distante :

- DNS : WINXP
- NetBios : VULNITLAB\WINXP

Services :

- 137/udp : Netbios name service - non testé
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing

### **VULNITLAB\SQL2K5 (192.168.1.54)**

Date de dernier scan : 2011-12-07 15:30:03

Compte administrateur validé : non

Cible testée : oui

Nombre de vulnérabilités :

- Critique : 1
- Majeur : 1
- Élevé : 1
- Ports ouverts : 5

Informations sur la machine distante :

- DNS : sql2k5
- NetBios : VULNITLAB\SQL2K5

Services :

- 135/tcp : RPC - Microsoft EPMAP - non testé
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing
- 1027/tcp : exosee - non testé
- 1433/tcp : MSSQL - Microsoft SQL Server

## **Résumé**

- WORKGROUP\OWASPBWA (192.168.1.21) - Contrôle d'accès / Compte Auth. Trivial



- Critique
- WORKGROUP\OWASPBWA (192.168.1.21) - Patch mgt / Application des correctifs Unix - Critique
- WORKGROUP\OWASPBWA (192.168.1.21) - Développement / SQLi - Critique
- WORKGROUP\OWASPBWA (192.168.1.21) - Patch mgt / Application des correctifs Web - Critique
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [device] L'appareil a des droits publics. - Majeur
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [account] Mauvais droits sur le dossier parent du home. - Majeur
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [permissions] Le fichier est setgid. - Majeur
- WORKGROUP\OWASPBWA (192.168.1.21) - Développement / XSS - Majeur
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / Liste d'utilisateurs accessible - Élevé
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / Fingerprint BD - Élevé
- WORKGROUP\OWASPBWA (192.168.1.21) - Développement / FI - Élevé
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / Capture de MDP - Élevé
- WORKGROUP\OWASPBWA (192.168.1.21) - Développement / CSRF - Élevé
- WORKGROUP\ORA9I (192.168.1.36) - Contrôle d'accès / Mot de passe trivial - Critique
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Application des correctifs de bases de données - Critique
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Application des correctifs Windows - Critique
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Application des correctifs Web - Critique
- WORKGROUP\ORA9I (192.168.1.36) - Chiffrement / Service FTP - Élevé
- WORKGROUP\ORA9I (192.168.1.36) - Configuration / Liste d'instances accessible - Élevé
- WORKGROUP\ORA9I (192.168.1.36) - Chiffrement / Chiffrement faible - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Mot de passe trivial - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Liste d'utilisateurs accessible - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Dossier partagé publiquement accessible - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Communauté SNMP en écriture - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Application des correctifs Windows - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Informations par RPC - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Service Discard - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Communauté SNMP publique - Critique
- VULNITLAB\SQL2K (192.168.1.45) - Contrôle d'accès / Relai mail ouvert - Élevé
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Application des correctifs Web - Élevé
- VULNITLAB\SQL2K5 (192.168.1.54) - Patch mgt / Application des correctifs Windows - Critique
- VULNITLAB\SQL2K5 (192.168.1.54) - Patch mgt / Application des correctifs de bases de données - Majeur
- VULNITLAB\SQL2K5 (192.168.1.54) - Configuration / Liste d'instances accessible - Élevé
- VULNITLAB\WINXP (192.168.1.84) - Patch mgt / Application des correctifs Windows - Critique
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Logiciel désactivé - Majeur
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Exigences de complexité des mots de passe désactivées - Majeur
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Longueur minimale des mots de passe trop courte - Majeur



- VULNITLAB\WINXP (192.168.1.84) - Configuration / Compte local activé - Majeur
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Mot de passe n'expirant jamais - Majeur



## WORKGROUP\OWASPBWA (192.168.1.21)

### Contrôle d'accès / Compte Auth. Trivial

Critique

**Description :** Un compte d'authentification trivial a été découvert sur cette page Internet.

**Résolution :** Changer le mot de passe de ce compte en choisissant un mot de passe complexe.

**Priorité :** Critique

**Méthodologie :** boîte noire

**Risque :** 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Références :** [OWASP 2010 A9](#), [OWASP prevention sheet](#), [CWE-521](#)

- Page : <http://192.168.1.21/mutillidae/index.php?page=login.php>  
Méthode : POST  
Informations : [POST(Fuzz) - <http://192.168.1.21/mutillidae/index.php?page=login.php>  
Params: {#user\_name:admin#password:admin#Submit\_button:Submit}]
- Page : <http://192.168.1.21/mutillidae/index.php?page=user-info.php>  
Méthode : POST  
Informations : [POST(Fuzz) - <http://192.168.1.21/mutillidae/index.php?page=user-info.php>  
Params: {#view\_user\_name:admin#password:admin#Submit\_button:Submit}]
- Page : <http://192.168.1.21/WackoPicko/admin/index.php?page=login>  
Méthode : POST  
Informations : [POST(Fuzz) - <http://192.168.1.21/WackoPicko/admin/index.php?page=login>  
Params: {#adminname:admin#password:admin}  
Cookies: {%PHPSESSID:k56vbc1uf3dnabf5kcdbcecoc5}]

### Patch mgt / Application des correctifs Unix

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte blanche

- Correctif manquant : [USN-1210-1](#)  
Résumé : Ubuntu Update for firefox USN-1210-1  
Script de test et informations relatives à cette vulnérabilité : [840756](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-2999](#), [CVE-2011-3000](#), [CVE-2011-2996](#), [CVE-2011-2372](#), [CVE-2011-3001](#), [CVE-2011-2995](#)
- Correctif manquant : [USN-1184-1](#)  
Résumé : Ubuntu Update for firefox USN-1184-1  
Script de test et informations relatives à cette vulnérabilité : [840727](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-2984](#), [CVE-2011-2982](#), [CVE-2011-2378](#), [CVE-2011-2981](#), [CVE-2011-0084](#), [CVE-2011-2983](#)
- Correctif manquant : [USN-1263-2](#)  
Résumé : Ubuntu Update for openjdk-6 USN-1263-2  
Script de test et informations relatives à cette vulnérabilité : [840872](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-3551](#), [CVE-2011-3521](#), [CVE-2011-3548](#), [CVE-2011-3547](#), [CVE-2011-3544](#), [CVE-2011-3560](#), [CVE-2011-3556](#), [CVE-2011-3557](#), [CVE-2011-3554](#), [CVE-2011-3558](#), [CVE-2011-3389](#), [CVE-2011-3552](#), [CVE-2011-3553](#)
- Packet affecté : -SUN JAVA JRE/JDK  
Résumé : Sun Java JRE Multiple Vulnerabilities (Linux)



- Script de test et informations relatives à cette vulnérabilité : [902168](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2010-1423](#) , [CVE-2010-0886](#) , [CVE-2010-0887](#)
- Correctif manquant : [USN-1010-1](#)  
 Résumé : Ubuntu Update for openjdk-6, openjdk-6b18 vulnerabilities USN-1010-1  
 Script de test et informations relatives à cette vulnérabilité : [840527](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2009-3555](#) , [CVE-2010-3554](#) , [CVE-2010-3553](#) , [CVE-2010-3557](#) , [CVE-2010-3562](#) , [CVE-2010-3551](#) , [CVE-2010-3573](#) , [CVE-2010-3549](#) , [CVE-2010-3566](#) , [CVE-2010-3569](#) , [CVE-2010-3565](#) , [CVE-2010-3568](#) , [CVE-2010-3574](#) , [CVE-2010-3548](#) , [CVE-2010-3564](#) , [CVE-2010-3541](#) , [CVE-2010-3567](#) , [CVE-2010-3561](#)
  - Correctif manquant : [USN-1049-2](#)  
 Résumé : Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1049-2  
 Script de test et informations relatives à cette vulnérabilité : [840609](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-0054](#) , [CVE-2011-0057](#) , [CVE-2011-0058](#) , [CVE-2011-0056](#) , [CVE-2011-0055](#) , [CVE-2011-0053](#) , [CVE-2011-0061](#) , [CVE-2010-1585](#) , [CVE-2011-0062](#) , [CVE-2011-0051](#) , [CVE-2011-0059](#)
  - Correctif manquant : [USN-1154-1](#)  
 Résumé : Ubuntu Update for openjdk-6 USN-1154-1  
 Script de test et informations relatives à cette vulnérabilité : [840683](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-0872](#) , [CVE-2011-0870](#) , [CVE-2011-0864](#) , [CVE-2011-0868](#) , [CVE-2011-0869](#) , [CVE-2011-0815](#) , [CVE-2011-0871](#) , [CVE-2011-0822](#) , [CVE-2011-0867](#) , [CVE-2011-0862](#) , [CVE-2011-0865](#)
  - Correctif manquant : [USN-1112-1](#)  
 Résumé : Ubuntu Update for firefox USN-1112-1  
 Script de test et informations relatives à cette vulnérabilité : [840640](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-0071](#) , [CVE-2011-0070](#) , [CVE-2011-0065](#) , [CVE-2011-1202](#) , [CVE-2011-0075](#) , [CVE-2011-0080](#) , [CVE-2011-0081](#) , [CVE-2011-0074](#) , [CVE-2011-0077](#) , [CVE-2011-0072](#) , [CVE-2011-0073](#) , [CVE-2011-0069](#) , [CVE-2011-0067](#) , [CVE-2011-0078](#) , [CVE-2011-0066](#)
  - Correctif manquant : [USN-1149-1](#)  
 Résumé : Ubuntu Update for firefox USN-1149-1  
 Script de test et informations relatives à cette vulnérabilité : [840684](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-0083](#) , [CVE-2011-2374](#) , [CVE-2011-2373](#) , [CVE-2011-0085](#) , [CVE-2011-2371](#) , [CVE-2011-2365](#) , [CVE-2011-2377](#) , [CVE-2011-2376](#) , [CVE-2011-2362](#) , [CVE-2011-2364](#) , [CVE-2011-2363](#)
  - Correctif manquant : [USN-1000-1](#)  
 Résumé : Ubuntu Update for Linux kernel vulnerabilities USN-1000-1  
 Script de test et informations relatives à cette vulnérabilité : [840523](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2009-4895](#) , [CVE-2010-2066](#) , [CVE-2010-3078](#) , [CVE-2010-2954](#) , [CVE-2010-2955](#) , [CVE-2010-3904](#) , [CVE-2010-2963](#) , [CVE-2010-2521](#) , [CVE-2010-2942](#) , [CVE-2010-3477](#) , [CVE-2010-3080](#) , [CVE-2010-2495](#) , [CVE-2010-3705](#) , [CVE-2010-3437](#) , [CVE-2010-2524](#) , [CVE-2010-3067](#) , [CVE-2010-2226](#) , [CVE-2010-3084](#) , [CVE-2010-3310](#) , [CVE-2010-2478](#) , [CVE-2010-2248](#) , [CVE-2010-3442](#) , [CVE-2010-2798](#) , [CVE-2010-3432](#) , [CVE-2010-2946](#) , [CVE-2010-2960](#) , [CVE-2010-3015](#)
  - Correctif manquant : [USN-1079-1](#)  
 Résumé : Ubuntu Update for openjdk-6 vulnerabilities USN-1079-1  
 Script de test et informations relatives à cette vulnérabilité : [840607](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2010-4469](#) , [CVE-2010-4472](#) , [CVE-2010-4448](#) , [CVE-2010-4450](#) , [CVE-2010-4471](#) , [CVE-2011-0706](#) , [CVE-2010-4476](#) , [CVE-2010-4470](#) , [CVE-2010-4465](#)
  - Correctif manquant : [USN-1049-1](#)  
 Résumé : Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1049-1  
 Script de test et informations relatives à cette vulnérabilité : [840604](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-0054](#) , [CVE-2011-0057](#) , [CVE-2011-0058](#) , [CVE-2011-0056](#) , [CVE-2011-0055](#) , [CVE-2011-0053](#) , [CVE-2011-0061](#) , [CVE-2010-1585](#) , [CVE-2011-0062](#) , [CVE-2011-0051](#) , [CVE-2011-0059](#)
  - Correctif manquant : [USN-1263-1](#)  
 Résumé : Ubuntu Update for icedtea-web USN-1263-1  
 Script de test et informations relatives à cette vulnérabilité : [840805](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/A:C/).  
 Références : [CVE-2011-3551](#) , [CVE-2011-3521](#) , [CVE-2011-3548](#) , [CVE-2011-3547](#) , [CVE-2011-3544](#) , [CVE-2011-3560](#) , [CVE-2011-3556](#) , [CVE-2011-3557](#) , [CVE-2011-3554](#) , [CVE-](#)



- [2011-3558](#), [CVE-2011-3389](#), [CVE-2011-3552](#), [CVE-2011-3553](#)  
Correctif manquant : [USN-1267-1](#)  
Résumé : Ubuntu Update for freetype USN-1267-1  
Script de test et informations relatives à cette vulnérabilité : [840810](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-3439](#), [CVE-2011-3256](#)
- Correctif manquant : [USN-1019-1](#)  
Résumé : Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1019-1  
Script de test et informations relatives à cette vulnérabilité : [840553](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3776](#), [CVE-2010-3773](#), [CVE-2010-3772](#), [CVE-2010-3770](#), [CVE-2010-3775](#), [CVE-2010-3777](#), [CVE-2010-3768](#), [CVE-2010-3767](#), [CVE-2010-3766](#), [CVE-2010-3778](#), [CVE-2010-3771](#), [CVE-2010-3774](#)
- Correctif manquant : [USN-1085-1](#)  
Résumé : Ubuntu Update for tiff vulnerabilities USN-1085-1  
Script de test et informations relatives à cette vulnérabilité : [840610](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-2630](#), [CVE-2010-2595](#), [CVE-2010-2597](#), [CVE-2010-2598](#), [CVE-2011-0191](#), [CVE-2011-0192](#), [CVE-2010-2482](#), [CVE-2010-2483](#), [CVE-2010-3087](#)
- Correctif manquant : [USN-1251-1](#)  
Résumé : Ubuntu Update for firefox USN-1251-1  
Script de test et informations relatives à cette vulnérabilité : [840801](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-3004](#), [CVE-2011-3650](#), [CVE-2011-3647](#), [CVE-2011-3648](#)
- Correctif manquant : [USN-1334-1](#)  
Résumé : Ubuntu Update for libxml2 USN-1334-1  
Script de test et informations relatives à cette vulnérabilité : [840868](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-3905](#), [CVE-2011-3919](#), [CVE-2011-2821](#), [CVE-2011-0216](#), [CVE-2011-2834](#)
- Correctif manquant : [USN-1011-3](#)  
Résumé : Ubuntu Update for Xulrunner vulnerability USN-1011-3  
Script de test et informations relatives à cette vulnérabilité : [840528](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3765](#)
- Correctif manquant : [USN-1013-1](#)  
Résumé : Ubuntu Update for freetype vulnerabilities USN-1013-1  
Script de test et informations relatives à cette vulnérabilité : [840532](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3311](#), [CVE-2010-3814](#), [CVE-2010-3855](#)
- Correctif manquant : [USN-997-1](#)  
Résumé : Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-997-1  
Script de test et informations relatives à cette vulnérabilité : [840518](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3177](#), [CVE-2010-3182](#), [CVE-2010-3178](#), [CVE-2010-3176](#), [CVE-2010-3175](#), [CVE-2010-3179](#), [CVE-2010-3180](#), [CVE-2010-3183](#)
- Correctif manquant : [USN-1085-2](#)  
Résumé : Ubuntu Update for tiff regression USN-1085-2  
Script de test et informations relatives à cette vulnérabilité : [840613](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-2630](#), [CVE-2010-2595](#), [CVE-2010-2597](#), [CVE-2010-2598](#), [CVE-2011-0191](#), [CVE-2010-2482](#), [CVE-2010-3087](#)
- Correctif manquant : [USN-1153-1](#)  
Résumé : Ubuntu Update for libxml2 USN-1153-1  
Script de test et informations relatives à cette vulnérabilité : [840679](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-1944](#)
- Résumé : Perl Safe Module 'reval()' and 'rdo()' CVE-2010-1447 Restriction-Bypass Vulnerabilities  
Script de test et informations relatives à cette vulnérabilité : [100673](#)  
Risque : 8.5 (Impact : 10.0, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).  
Références : [CVE-2010-1447](#)
- Correctif manquant : [USN-1129-1](#)  
Résumé : Ubuntu Update for perl USN-1129-1  
Script de test et informations relatives à cette vulnérabilité : [840647](#)  
Risque : 8.5 (Impact : 10.0, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).  
Références : [CVE-2011-1487](#), [CVE-2010-4411](#), [CVE-2010-1168](#), [CVE-2010-2761](#), [CVE-2010-4410](#), [CVE-2010-1447](#)
- Correctif manquant : [USN-1012-1](#)



- Résumé : Ubuntu Update for cups, cupsys vulnerability USN-1012-1  
 Script de test et informations relatives à cette vulnérabilité : [840531](#)  
 Risque : 7.9 (Impact : 10.0, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-2941](#)
- Correctif manquant : [USN-1041-1](#)  
 Résumé : Ubuntu Update for linux, linux-ec2 vulnerabilities USN-1041-1  
 Script de test et informations relatives à cette vulnérabilité : [840565](#)  
 Risque : 7.9 (Impact : 9.2, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:N/).  
 Références : [CVE-2010-3296](#), [CVE-2010-3301](#), [CVE-2010-3861](#), [CVE-2010-3297](#), [CVE-2010-2943](#), [CVE-2010-3858](#), [CVE-2010-2537](#), [CVE-2010-2538](#), [CVE-2010-3298](#), [CVE-2010-4072](#), [CVE-2010-2962](#), [CVE-2010-3079](#)
  - Correctif manquant : [USN-1199-1](#)  
 Résumé : Ubuntu Update for apache2 USN-1199-1  
 Script de test et informations relatives à cette vulnérabilité : [840734](#)  
 Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2011-3192](#)
  - Résumé : Apache httpd Web Server Range Header Denial of Service Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [901203](#)  
 Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2011-3192](#)
  - Correctif manquant : [USN-1088-1](#)  
 Résumé : Ubuntu Update for krb5 vulnerability USN-1088-1  
 Script de test et informations relatives à cette vulnérabilité : [840616](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-0284](#)
  - Correctif manquant : [USN-1335-1](#)  
 Résumé : Ubuntu Update for t1lib USN-1335-1  
 Script de test et informations relatives à cette vulnérabilité : [840866](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-2642](#), [CVE-2011-1554](#), [CVE-2011-1553](#), [CVE-2011-1552](#)
  - Correctif manquant : [USN-1082-1](#)  
 Résumé : Ubuntu Update for pango1.0 vulnerabilities USN-1082-1  
 Script de test et informations relatives à cette vulnérabilité : [840602](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0421](#), [CVE-2011-0064](#), [CVE-2011-0020](#)
  - Correctif manquant : [USN-1126-2](#)  
 Résumé : Ubuntu Update for php5 USN-1126-2  
 Script de test et informations relatives à cette vulnérabilité : [840636](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2006-7243](#), [CVE-2011-1464](#), [CVE-2011-1471](#), [CVE-2011-1468](#), [CVE-2011-1469](#), [CVE-2010-4698](#), [CVE-2011-1072](#), [CVE-2011-1092](#), [CVE-2011-1466](#), [CVE-2011-1153](#), [CVE-2011-0441](#), [CVE-2010-4697](#), [CVE-2011-0420](#), [CVE-2011-0421](#), [CVE-2011-0708](#), [CVE-2011-1144](#), [CVE-2011-1148](#), [CVE-2011-1467](#), [CVE-2011-1470](#)
  - Packet affecté : -SUN JAVA SE JRE  
 Résumé : Oracle Java SE Multiple Vulnerabilities (Linux)  
 Script de test et informations relatives à cette vulnérabilité : [800500](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2009-3555](#), [CVE-2010-0840](#), [CVE-2010-0844](#), [CVE-2010-0092](#), [CVE-2010-0093](#), [CVE-2010-0838](#), [CVE-2010-0084](#), [CVE-2010-0843](#), [CVE-2010-0837](#), [CVE-2010-0088](#), [CVE-2010-0090](#), [CVE-2010-0848](#), [CVE-2010-0082](#), [CVE-2010-0095](#), [CVE-2010-0839](#), [CVE-2010-0094](#), [CVE-2010-0842](#), [CVE-2010-0087](#), [CVE-2010-0846](#), [CVE-2010-0085](#), [CVE-2010-0091](#), [CVE-2010-0847](#), [CVE-2010-0849](#), [CVE-2010-0089](#), [CVE-2010-0841](#), [CVE-2010-0845](#)
  - Packet affecté : -SAFE  
 Résumé : Perl Safe Module 'reval()' and 'rdo()' Restriction-Bypass Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [100672](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2010-1168](#)
  - Correctif manquant : [USN-1231-1](#)  
 Résumé : Ubuntu Update for php5 USN-1231-1  
 Script de test et informations relatives à cette vulnérabilité : [840782](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2010-1914](#), [CVE-2011-2202](#), [CVE-2011-2483](#), [CVE-2011-1938](#), [CVE-2011-3267](#), [CVE-2010-2484](#), [CVE-2011-1657](#), [CVE-2011-3182](#)
  - Packet affecté : -SAMBA  
 Résumé : Samba SID Parsing Remote Buffer Overflow Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [100803](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2010-3069](#)



- Correctif manquant : [USN-1108-2](#)  
Résumé : Ubuntu Update for dhcp3 USN-1108-2  
Script de test et informations relatives à cette vulnérabilité : [840645](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2011-0997](#)
- Correctif manquant : [USN-1007-1](#)  
Résumé : Ubuntu Update for nss vulnerabilities USN-1007-1  
Script de test et informations relatives à cette vulnérabilité : [840520](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2010-3170](#) , [CVE-2010-3173](#)
- Correctif manquant : [USN-1126-1](#)  
Résumé : Ubuntu Update for php5 USN-1126-1  
Script de test et informations relatives à cette vulnérabilité : [840646](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2006-7243](#) , [CVE-2011-1464](#) , [CVE-2011-1471](#) , [CVE-2011-1468](#) , [CVE-2011-1469](#) , [CVE-2010-4698](#) , [CVE-2011-1072](#) , [CVE-2011-1092](#) , [CVE-2011-1466](#) , [CVE-2011-1153](#) , [CVE-2011-0441](#) , [CVE-2010-4697](#) , [CVE-2011-0420](#) , [CVE-2011-0421](#) , [CVE-2011-0708](#) , [CVE-2011-1144](#) , [CVE-2011-1148](#) , [CVE-2011-1467](#) , [CVE-2011-1470](#)
- Correctif manquant : [USN-1158-1](#)  
Résumé : Ubuntu Update for curl USN-1158-1  
Script de test et informations relatives à cette vulnérabilité : [840685](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2011-2192](#) , [CVE-2009-2417](#) , [CVE-2010-0734](#)
- Correctif manquant : [USN-1252-1](#)  
Résumé : Ubuntu Update for tomcat6 USN-1252-1  
Script de test et informations relatives à cette vulnérabilité : [840803](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2011-3190](#) , [CVE-2011-2204](#) , [CVE-2011-2526](#)
- Correctif manquant : [USN-1108-1](#)  
Résumé : Ubuntu Update for dhcp3 vulnerability USN-1108-1  
Script de test et informations relatives à cette vulnérabilité : [840633](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2011-0997](#)
- Correctif manquant : [USN-1009-1](#)  
Résumé : Ubuntu Update for glibc, eglibc vulnerabilities USN-1009-1  
Script de test et informations relatives à cette vulnérabilité : [840525](#)  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3847](#) , [CVE-2010-3856](#)
- Correctif manquant : [USN-1080-1](#)  
Résumé : Ubuntu Update for linux vulnerabilities USN-1080-1  
Script de test et informations relatives à cette vulnérabilité : [840600](#)  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-4248](#) , [CVE-2010-4527](#) , [CVE-2010-3875](#) , [CVE-2010-4526](#) , [CVE-2010-4346](#) , [CVE-2010-4343](#) , [CVE-2010-3865](#) , [CVE-2010-4649](#) , [CVE-2011-1044](#) , [CVE-2010-3877](#) , [CVE-2010-3876](#) , [CVE-2010-3880](#)
- Correctif manquant : [USN-1009-2](#)  
Résumé : Ubuntu Update for eglibc, glibc vulnerability USN-1009-2  
Script de test et informations relatives à cette vulnérabilité : [840567](#)  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3847](#) , [CVE-2010-3856](#)

## Développement / SQLi

Critique

**Description :** Une injection SQL permet de duper le fonctionnement d'une page Internet afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées. Une injection SQL réussie permet de lire des informations sensibles d'une base de données, modifier son contenu, exécuter des opérations d'administration, récupérer le contenu d'un fichier présent dans le système de gestion de la base de données, voire dans le système d'exploitation.

**Résolution :** Contrôler et protéger les requêtes ou commandes SQL en utilisant des requêtes paramétrées ou en échappant les informations fournies par l'utilisateur.

**Priorité :** Critique



## Méthodologie : boîte noire

**Risque** : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Références** : [OWASP 2010 A1](#), [OWASP prevention sheet](#), [CWE-89](#)

- Page : <http://192.168.1.21/mutillidae/index.php?page=register.php>  
Méthode : POST  
Paramètre attaqué : user\_name  
Informations : user\_name=-6715' OR 1607=BENCHMARK(6000000,MD5(Char(100,73,81,119))) AND 'VULNITsaqnA'='VULNITsaqnA
- Page : <http://192.168.1.21/mutillidae/index.php?page=login.php>  
Méthode : POST  
Paramètre attaqué : user\_name  
Informations : user\_name=-3064' OR 5916=BENCHMARK(6000000,MD5(Char(65,102,108,122))) AND 'VULNITsxeUG'='VULNITsxeUG
- Page : <http://192.168.1.21/mutillidae/index.php?page=user-info.php>  
Méthode : POST  
Paramètre attaqué : view\_user\_name  
Informations : view\_user\_name=-1165' OR 2626=BENCHMARK(6000000,MD5(Char(116,109,65,77))) AND 'VULNITsyayF'='VULNITsyayF
- Page : <http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php>  
Méthode : POST  
Paramètre attaqué : show\_only\_user  
Informations : show\_only\_user=-6360' OR 5524=BENCHMARK(6000000,MD5(Char(109,100,77,67))) AND 'VULNITsuxPd'='VULNITsuxPd
- Page : <http://192.168.1.21/mutillidae/redirectandlog.php>  
Méthode : GET  
Paramètre attaqué : forwardurl  
Informations : forwardurl=-6036' OR 7735=SLEEP(6) AND 'VULNITsatyF'='VULNITsatyF
- Page : <http://192.168.1.21/mutillidae/index.php>  
Méthode : GET  
Paramètre attaqué : uid  
Cookie : uid=1  
Informations : [Cookie -> -4093' OR 6668=SLEEP(6) AND 'VULNITsIKow'='VULNITsIKow]
- Page : <http://192.168.1.21/mutillidae/index.php?page=dns-lookup.php>  
Méthode : POST  
Paramètre attaqué : uid  
Cookie : uid=1  
Informations : [Cookie -> -8329' OR 721=SLEEP(6) AND 'VULNITsTnUG'='VULNITsTnUG]
- Page : <http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php>  
Méthode : POST  
Paramètre attaqué : uid  
Cookie : uid=1  
Informations : [Cookie -> -184' OR 1192=SLEEP(6) AND 'VULNITsPenH'='VULNITsPenH]
- Page : <http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php>  
Méthode : POST  
Paramètre attaqué : uid  
Cookie : uid=1  
Informations : [Cookie -> -9448' OR 9272=SLEEP(6) AND 'VULNITsVtDw'='VULNITsVtDw]
- Page : <http://192.168.1.21/WackoPicko/users/login.php>  
Méthode : POST  
Paramètre attaqué : username  
Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5  
Informations : username=-8709' OR 7409=SLEEP(6) AND 'VULNITsUMIJ'='VULNITsUMIJ
- Page : <http://192.168.1.21/vicnum/vicnum5.php>  
Méthode : POST  
Paramètre attaqué : player  
Informations : player=-7453' OR 6591=SLEEP(6) AND 'VULNITsQEzb'='VULNITsQEzb

## Patch mgt / Application des correctifs Web

Critique

**Description** : Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement



installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte blanche

- Packet affecté : -WORDPRESS  
Résumé : WordPress 'wp-admin' Multiple Vulnerabilities - Aug09  
Script de test et informations relatives à cette vulnérabilité : [900915](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-2853](#) , [CVE-2009-2854](#)
- Packet affecté : -WORDPRESS  
Résumé : WordPress cat Parameter Directory Traversal Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [800124](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2008-4769](#)
- Packet affecté : -WORDPRESS  
Résumé : WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [900183](#)  
Risque : 8.5 (Impact : 10.0, Exploitabilité : 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).  
Références : [CVE-2008-5695](#)
- Packet affecté : - OF WORDPRESS  
Résumé : WordPress Multiple Vulnerabilities  
Script de test et informations relatives à cette vulnérabilité : [900219](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2008-3747](#)
- Packet affecté : -PHP  
Résumé : PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [100684](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
Références : [CVE-2010-2225](#)

### Configuration / [device] L'appareil a des droits publics.

**Majeur**

**Description :** Les devices ayant des droits inappropriés (world) peuvent être accédés par n'importe quel utilisateur système. Cela peut ouvrir des brèches de sécurité si ce sont des devices partagés ou des binaires maintenus (des disques par exemple).

**Résolution :** L'administrateur devrait mettre correctement les accès au devices (en utilisant la configuration de groupe pour fournir un accès au device pour plusieurs utilisateurs, par exemple).

**Priorité :** Majeur

**Méthodologie :** boîte blanche

**Risque :** 8.7 (Impact : 9.5, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:P/I:C/A:C/).

**Informations :** [/dev/fuse, /dev/log, /dev/ptmx, /dev/rfkill]

### Configuration / [account] Mauvais droits sur le dossier parent du home.

**Majeur**

**Description :** Le dossier home du compte affiché a le droit d'écriture de groupe, droit d'écriture pour tous - ou les deux - activé. Cela permet d'ajouter aux autres comptes de nouveaux fichiers (et potentiellement de supprimer des fichiers).

**Résolution :** Les droits en écriture devrait être retirés.



**Priorité** : Majeur

**Méthodologie** : boîte blanche

**Risque** : 8.5 (Impact : 9.2, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:C/A:N/).

**Informations** : [Login ID mail's home directory (/var/mail) has group `mail' write access, Login ID polkituser's home directory (/var/run/PolicyKit) has group `polkituser' write access]

### Configuration / [permissions] Le fichier est setgid.

**Majeur**

**Description** : Le fichier indiqué a le bit setgid, mais ne devrais pas.

**Résolution** : Cela devrait être changé en utilisant 'chmod g-s fichier' où 'fichier' est le fichier indiqué. Le système devrait être vérifié pour des signes d'intrusion.

**Priorité** : Majeur

**Méthodologie** : boîte blanche

**Risque** : 8.5 (Impact : 9.2, Exploitabilité : 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:C/A:N/).

**Informations** :

- File: /usr/bin/at - Group: daemon
- File: /usr/bin/wall - Group: tty

### Développement / XSS

**Majeur**

**Description** : Une faille XSS permet à un attaquant d'exécuter un programme dans le navigateur d'un utilisateur ou visiteur, afin de détourner ses informations ou le rediriger vers des sites malveillants.

**Résolution** : S'assurer qu'aucune donnée saisie par l'utilisateur ne puisse être traitée par le navigateur comme du contenu exécutable.

**Priorité** : Majeur

**Méthodologie** : boîte noire

**Risque** : 8.3 (Impact : 8.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

**Références** : [OWASP 2010 A2](#), [OWASP prevention sheet](#), [CWE-79](#)

- Page : <http://192.168.1.21/vicnum/vicnum5.php>  
Méthode : POST  
Paramètre attaqué : player  
Informations : player=<script>alert(331559492711322129638300)</script>
- Page : <http://192.168.1.21/WackoPicko/piccheck.php>  
Méthode : POST  
Paramètre attaqué : name  
Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5  
Informations : name=<script>alert(331559492711322129319722)</script>
- Page : <http://192.168.1.21/WackoPicko/pictures/search.php>  
Méthode : GET  
Paramètre attaqué : query  
Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5  
Informations : query=<script>alert(331559492711322129318918)</script>
- Page : <http://192.168.1.21/mutilidae/index.php?page=login.php>  
Méthode : POST  
Paramètre attaqué : user\_name  
Informations : user\_name=<script>alert(331559492711322127789288)</script>
- Page : <http://192.168.1.21/mutilidae/index.php?page=user-info.php>  
Méthode : POST



<p>Paramètre attaqué : password Informations : password=&lt;script&gt;alert(331559492711322127790579)&lt;/script&gt;</p> <ul style="list-style-type: none"> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php">http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php</a> Méthode : POST Paramètre attaqué : input_from_form Informations : input_from_form=&lt;script&gt;alert(331559492711322127791956)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/WackoPicko/guestbook.php">http://192.168.1.21/WackoPicko/guestbook.php</a> Méthode : POST Paramètre attaqué : comment Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5 Informations : comment=&lt;script&gt;alert(331559492711322129321736)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=register.php">http://192.168.1.21/mutillidae/index.php?page=register.php</a> Méthode : POST Paramètre attaqué : password Informations : password=&lt;script&gt;alert(331559492711322127788820)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=register.php">http://192.168.1.21/mutillidae/index.php?page=register.php</a> Méthode : POST Paramètre attaqué : user_name Informations : user_name=&lt;script&gt;alert(331559492711322127788705)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=user-info.php">http://192.168.1.21/mutillidae/index.php?page=user-info.php</a> Méthode : POST Paramètre attaqué : view_user_name Informations : view_user_name=&lt;script&gt;alert(331559492711322127790383)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php">http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php</a> Méthode : POST Paramètre attaqué : show_only_user Informations : show_only_user=&lt;script&gt;alert(331559492711322127792521)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php">http://192.168.1.21/mutillidae/index.php</a> Méthode : GET Paramètre attaqué : php_file_name Informations : php_file_name=&lt;script&gt;alert(331559492711322127793620)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/vicnum/cgi-bin/vicnum1.pl">http://192.168.1.21/vicnum/cgi-bin/vicnum1.pl</a> Méthode : POST Paramètre attaqué : player Informations : player=&lt;script&gt;alert(331559492711322129637331)&lt;/script&gt;</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=login.php">http://192.168.1.21/mutillidae/index.php?page=login.php</a> Méthode : POST Paramètre attaqué : password Informations : password=&lt;script&gt;alert(331559492711322127789345)&lt;/script&gt;</li> </ul>
---

Configuration / Liste d'utilisateurs accessible	Élevé
<p><b>Description :</b> La configuration et la version du serveur permettent d'obtenir la liste de ses utilisateurs.</p> <p><b>Résolution :</b> Migrer vers un système d'exploitations plus récent.</p> <p><b>Priorité :</b> Élevé</p> <p><b>Méthodologie :</b> boîte noire</p> <p><b>Risque :</b> 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N).</p> <p><b>Informations :</b> [nobody, None, user, root]</p>	

Configuration / Fingerprint BD	Élevé
<p><b>Description :</b> Donner des informations sur le système de base de données utilisé peut aider un attaquant (message d'erreurs...)</p> <p><b>Résolution :</b> Ne pas afficher de message d'erreur donnant des informations sur la base utilisée</p>	



**Priorité** : Élevé

**Méthodologie** : boîte noire

**Risque** : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

- Page : <http://192.168.1.21/mutillidae/index.php>  
Méthode : GET  
Informations : An error showed that the DBMS could be MySQL
- Page : <http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php>  
Méthode : POST  
Informations : An error showed that the DBMS could be MySQL
- Page : <http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php>  
Méthode : POST  
Informations : An error showed that the DBMS could be MySQL
- Page : <http://192.168.1.21/mutillidae/index.php?page=dns-lookup.php>  
Méthode : POST  
Informations : An error showed that the DBMS could be MySQL
- Page : <http://192.168.1.21/mutillidae/>  
Méthode : GET  
Informations : An error showed that the DBMS could be MySQL

## Développement / FI

Élevé

**Description** : L'inclusion de fichiers permet à un attaquant d'envoyer un programme sur un serveur Internet ou de récupérer des informations de ce serveur.

**Résolution** : L'inclusion de fichiers peut être évitée en protégeant les références aux objets (internes ou externes) paramétrables. Elle peut également être restreinte par des configurations serveur appropriées.

**Priorité** : Élevé

**Méthodologie** : boîte noire

**Risque** : 7.3 (Impact : 9.5, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:P/I:C/A:C/).

**Références** : OWASP 2007 A3, CWE-98

- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php\\_file\\_name=vulnit-0.24966086147634248](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.24966086147634248)  
Paramètre attaqué : page  
Cookie : showhints=1
- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php\\_file\\_name=footer.php](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=footer.php)  
Paramètre attaqué : page
- Page : <http://192.168.1.21/mutillidae/?page=/etc/passwd>  
Paramètre attaqué : page
- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php\\_file\\_name=vulnit-0.2590453632606361](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.2590453632606361)  
Paramètre attaqué : page  
Cookie : uid=1
- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php\\_file\\_name=vulnit-0.9298311197090497](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.9298311197090497)  
Paramètre attaqué : page  
Cookie : uid=1;showhints=1
- Page : <http://192.168.1.21/mutillidae/index.php?page=/etc/passwd>  
Paramètre attaqué : page
- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php\\_file\\_name=vulnit-0.01902171156707999](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.01902171156707999)  
Paramètre attaqué : page
- Page : [http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php\\_file\\_name=/etc/passwd](http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=/etc/passwd)  
Paramètre attaqué : php\_file\_name
- Page : <http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php>  
Paramètre attaqué : text\_file\_name



Configuration / Capture de MDP	Élevé
<p><b>Description :</b> Le mot de passe d'un formulaire d'authentification transmis en HTTP (non chiffré) peut être intercepté et usurpé.</p> <p><b>Résolution :</b> Chiffrer la communication (en HTTPS).</p> <p><b>Priorité :</b> Élevé</p> <p><b>Méthodologie :</b> boîte noire</p> <p><b>Risque :</b> 7.3 (Impact : 9.2, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:C/).</p> <p><b>Références :</b> OWASP 2010 A9OWAP Prevention sheet, CWE-319</p> <ul style="list-style-type: none"> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=user-info.php">http://192.168.1.21/mutillidae/index.php?page=user-info.php</a> Paramètre attaqué : password</li> <li>• Page : <a href="http://192.168.1.21/bodgeit/register.jsp">http://192.168.1.21/bodgeit/register.jsp</a> Paramètre attaqué : password1 Cookie : JSESSIONID=9AAC0580FF9958EE4B5AF33FAAD75974</li> <li>• Page : <a href="http://192.168.1.21/WackoPicko/users/register.php">http://192.168.1.21/WackoPicko/users/register.php</a> Paramètre attaqué : password Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=register.php">http://192.168.1.21/mutillidae/index.php?page=register.php</a> Paramètre attaqué : password</li> <li>• Page : <a href="http://192.168.1.21/bodgeit/login.jsp">http://192.168.1.21/bodgeit/login.jsp</a> Paramètre attaqué : password Cookie : JSESSIONID=9AAC0580FF9958EE4B5AF33FAAD75974</li> <li>• Page : <a href="http://192.168.1.21/WackoPicko/admin/index.php?page=login">http://192.168.1.21/WackoPicko/admin/index.php?page=login</a> Paramètre attaqué : password Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5</li> <li>• Page : <a href="http://192.168.1.21/WackoPicko/users/login.php">http://192.168.1.21/WackoPicko/users/login.php</a> Paramètre attaqué : password Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5</li> <li>• Page : <a href="http://192.168.1.21/WackoPicko/passcheck.php">http://192.168.1.21/WackoPicko/passcheck.php</a> Paramètre attaqué : password Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5</li> <li>• Page : <a href="http://192.168.1.21/mutillidae/index.php?page=login.php">http://192.168.1.21/mutillidae/index.php?page=login.php</a> Paramètre attaqué : password</li> </ul>	

Développement / CSRF	Élevé
<p><b>Description :</b> Les attaques CSRF (ou XSRF) permettent un attaquant de faire exécuter des requêtes à l'utilisateur sans son consentement</p> <p><b>Résolution :</b> Protéger les formulaires en ajoutant un jeton avec une valeur non prédictible et vérifier cette valeur lors de la réception des données du formulaire</p> <p><b>Priorité :</b> Élevé</p> <p><b>Méthodologie :</b> boîte noire</p> <p><b>Risque :</b> 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).</p> <ul style="list-style-type: none"> <li>• Page : <a href="http://192.168.1.21/bodgeit/basket.jsp">http://192.168.1.21/bodgeit/basket.jsp</a> Méthode : GET Informations : Form: '&lt;form action="basket.jsp" method="post"&gt;&lt;/form&gt;' is vulnerable</li> </ul>	



## WORKGROUP\ORA9I (192.168.1.36)

### Contrôle d'accès / Mot de passe trivial

Critique

**Description :** L'accès à cette base de données Oracle dispose d'un ou plusieurs comptes triviaux (i.e. mot de passe publiquement connu, voir la liste des instances et comptes ci-dessous).

**Résolution :** Changer les mots de passe de ces comptes ou les verrouiller.

**Priorité :** Critique

**Méthodologie :** boîte noire

**Risque :** 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Informations :** SID : ORA9I ([DBSNMP/DBSNMP, SCOTT/TIGER, SYSTEM/ORACLE])

### Patch mgt / Application des correctifs de bases de données

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte noire

- Packet affecté : -ORACLE DATABASE AND APPLICATION SERVER  
 Résumé : Oracle Database Server and Application Server Ultra Search Component Unspecified Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [802524](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-0347](#)
- Packet affecté : -ORACLE DATABASE AND APPLICATION SERVER  
 Résumé : Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [802526](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2006-0282](#), [CVE-2006-0291](#), [CVE-2006-0285](#), [CVE-2006-0290](#), [CVE-2006-0283](#), [CVE-2006-0286](#), [CVE-2006-0287](#)
- Packet affecté : -ORACLE DATABASE  
 Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities - Jan 08  
 Script de test et informations relatives à cette vulnérabilité : [802528](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-0339](#), [CVE-2008-0340](#), [CVE-2008-0345](#), [CVE-2008-0341](#), [CVE-2008-0344](#), [CVE-2008-0343](#), [CVE-2008-0342](#)
- Packet affecté : -ORACLE DATABASE  
 Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [802527](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2006-0547](#), [CVE-2006-0586](#), [CVE-2006-0267](#), [CVE-2006-0270](#), [CVE-2006-0261](#), [CVE-2006-0271](#), [CVE-2006-0263](#), [CVE-2006-0272](#), [CVE-2006-0256](#), [CVE-2006-0552](#), [CVE-2006-0268](#), [CVE-2006-0262](#), [CVE-2006-0258](#), [CVE-2006-0259](#), [CVE-2006-0257](#), [CVE-2006-0551](#), [CVE-2006-0269](#), [CVE-2006-0260](#), [CVE-2006-0265](#), [CVE-2006-0266](#), [CVE-2006-0548](#), [CVE-2006-0549](#)
- Packet affecté : -ORACLE DATABASE  
 Résumé : Oracle Database Server Multiple Vulnerabilities - Oct 06  
 Script de test et informations relatives à cette vulnérabilité : [802520](#)  
 Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).  
 Références : [CVE-2006-5335](#), [CVE-2006-5342](#), [CVE-2006-5332](#), [CVE-2006-5343](#), [CVE-](#)



- 2006-5341, [CVE-2006-5344](#), [CVE-2006-5339](#), [CVE-2006-5334](#), [CVE-2006-5340](#), [CVE-2006-5333](#), [CVE-2006-5336](#), [CVE-2006-5345](#)

  - **Packet affecté :** -ORACLE DATABASE  
 Résumé : Oracle Database Server Multiple Unspecified Vulnerabilities - April 06  
 Script de test et informations relatives à cette vulnérabilité : [802538](#)  
 Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).  
 Références : [CVE-2006-1873](#), [CVE-2006-1874](#), [CVE-2006-1868](#), [CVE-2006-1872](#), [CVE-2006-1871](#)
  - **Packet affecté :** -ORACLE DATABASE  
 Résumé : Oracle Database Server MDSYS.MD Buffer Overflows and Denial of Service Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [802523](#)  
 Risque : 8.5 (Impact : 9.2, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:N/I:C/A:C/).  
 Références : [CVE-2007-0272](#)
  - **Packet affecté :** -ORACLE DATABASE  
 Résumé : Oracle Database Server 'RDBMS' component Denial of Service Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [802539](#)  
 Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2007-5506](#)
  - **Packet affecté :** Oracle 9iAS SOAP Default Configuration Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [11227](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2001-1371](#)
  - **Packet affecté :** -ORACLE DATABASE  
 Résumé : Oracle Database Server Upgrade and Downgrade Component Multiple Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [802519](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2007-2118](#), [CVE-2007-2113](#)
  - **Packet affecté :** -ORACLE DATABASE AND APPLICATION SERVER  
 Résumé : Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities  
 Script de test et informations relatives à cette vulnérabilité : [802525](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2006-0435](#)

## Patch mgt / Application des correctifs Windows

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte noire

- **Correctif manquant :** [MS10-012](#)  
 Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)  
 Script de test et informations relatives à cette vulnérabilité : [902269](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0022](#), [CVE-2010-0020](#), [CVE-2010-0021](#), [CVE-2010-0231](#)
- **Correctif manquant :** [MS09-001](#)  
 Résumé : Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote  
 Script de test et informations relatives à cette vulnérabilité : [900233](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-4835](#), [CVE-2008-4114](#), [CVE-2008-4834](#)
- **Correctif manquant :** [MS09-001](#)  
 Résumé : SMB Registry : Windows Service Pack version  
 Script de test et informations relatives à cette vulnérabilité : [10401](#)  
 Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-1999-0662](#)



## Patch mgt / Application des correctifs Web

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte noire

- Packet affecté : -OPENSSL  
Résumé : OpenSSL 'bn\_wexpend()' Error Handling Unspecified Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [100527](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C).  
Références : [CVE-2009-3245](#)
- Packet affecté : -OPENSSL  
Résumé : OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [100668](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P).  
Références : [CVE-2010-0742](#)
- Résumé : mod\_ssl hook functions format string vulnerability  
Script de test et informations relatives à cette vulnérabilité : [13651](#)  
Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P).  
Références : [CVE-2004-0700](#)

## Chiffrement / Service FTP

Élevé

**Description :** Le transfert de fichier par FTP n'est pas chiffré. Les identifiants de connexion ainsi que les données transférées peuvent donc être interceptés et utilisés par une personne mal intentionnée.

**Résolution :** Utiliser une solution chiffrée de transfert de fichiers (par exemple, SFTP).

**Priorité :** Élevé

**Méthodologie :** boîte noire

**Risque :** 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N).

## Configuration / Liste d'instances accessible

Élevé

**Description :** La configuration de la base de données Oracle permet d'obtenir la liste des instances de bases de données.

**Résolution :** Migrer vers une version plus récente (Oracle 10g minimum) et s'assurer que le fichier listener.ora ne contient pas la ligne "LOCAL\_OS\_AUTHENTICATION\_LISTENER = OFF".

**Priorité :** Élevé

**Méthodologie :** boîte noire

**Risque :** 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N).

**Informations :** [ORA9I]

## Chiffrement / Chiffrement faible

Élevé



**Description :** Le serveur SSL accepte des connexions utilisant des algorithmes de chiffrement faibles (dont la longueur de clé est inférieure à 128 bits), ce qui pourrait permettre de déchiffrer en un temps raisonnable les identifiants de connexion et données transmises sur le réseau.

**Résolution :** Restreindre le choix d'algorithmes de chiffrement aux seuls algorithmes dont les clés sont au moins de longueur 128 bits.

**Priorité :** Élevé

**Méthodologie :** boîte noire

**Risque :** 7.1 (Impact : 9.2, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:N/).

**Informations :** DES-CBC-MD5 (SSLv2 - 56 bits), EXP-RC4-MD5 (SSLv2 - 40 bits), EDH-RSA-DES-CBC-SHA (SSLv3 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (SSLv3 - 40 bits), DES-CBC-SHA (SSLv3 - 56 bits), EXP-DES-CBC-SHA (SSLv3 - 40 bits), EXP-RC4-MD5 (SSLv3 - 40 bits), EDH-RSA-DES-CBC-SHA (TLSv1 - 56 bits), EXP-EDH-RSA-DES-CBC-SHA (TLSv1 - 40 bits), DES-CBC-SHA (TLSv1 - 56 bits), EXP-DES-CBC-SHA (TLSv1 - 40 bits), EXP-RC4-MD5 (TLSv1 - 40 bits)

**VULNITLAB\SQL2K (192.168.1.45)****Contrôle d'accès / Mot de passe trivial****Critique**

**Description :** L'accès à cette base de données Microsoft SQL Server dispose d'un compte administrateur trivial (i.e. mot de passe nul ou identique à l'identifiant).

**Résolution :** Modifier le mot de passe du compte administrateur.

**Priorité :** Critique

**Méthodologie :** boîte noire

**Risque :** 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Informations :** SID : /1433 ([sa])

**Configuration / Liste d'utilisateurs accessible****Critique**

**Description :** La configuration et la version du serveur permettent d'obtenir la liste de ses utilisateurs.

**Résolution :** Migrer vers un système d'exploitations plus récent.

**Priorité :** Critique

**Méthodologie :** boîte noire

**Risque :** 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

**Informations :** [Administrator, Guest, IUSR\_VULNITSMB, IWAM\_VULNITSMB, ToBeFound, TsInternetUser]

**Contrôle d'accès / Dossier partagé publiquement accessible****Critique**

**Description :** La configuration actuelle permet à tout un chacun (disposant ou non d'un compte sur le domaine) d'accéder aux partages Windows et aux fichiers qu'ils contiennent.

**Résolution :** Restreindre l'accès à ce partage aux seuls utilisateurs autorisés.

**Priorité :** Critique

**Méthodologie :** boîte noire

**Risque :** 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Informations :** [TESTSMB]

**Configuration / Communauté SNMP en écriture****Critique**

**Description :** La communauté SNMP décrite ci-dessous est accessible à tous en écriture, ce qui permet d'administrer le serveur à distance (et en particulier l'arrêter).

**Résolution :** Migrer vers SNMP v3 pour ajouter une authentification. A défaut, changer le nom de la communauté ou restreindre les machines habilitées à accéder au service SNMP.

**Priorité :** Critique



**Méthodologie** : boîte noire

**Risque** : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

**Informations** : [private]

### Patch mgt / Application des correctifs Windows

Critique

**Description** : Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution** : Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité** : Critique

**Méthodologie** : boîte noire

- Correctif manquant : [MS10-012](#)  
Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)  
Script de test et informations relatives à cette vulnérabilité : [902269](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
- Résumé : IIS .IDA ISAPI filter applied  
Script de test et informations relatives à cette vulnérabilité : [10695](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2001-0500](#)
- Correctif manquant : [MS11-035](#)  
Résumé : Microsoft Windows WINS Remote Code Execution Vulnerability (2524426)  
Script de test et informations relatives à cette vulnérabilité : [802260](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:I/C/A:C/).  
Références : [CVE-2011-1248](#)

### Configuration / Informations par RPC

Critique

**Description** : Un service RPC fournit à tout un chacun (disposant ou non d'un compte sur le domaine) de nombreuses informations précieuses sur le système.

**Résolution** : Ce service requiert un compte (local ou domaine) à partir de votre système d'exploitation.

**Priorité** : Critique

**Méthodologie** : boîte noire

**Risque** : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

**Informations** : Voici un échantillon d'informations utiles pouvant être collectées par RPC :

- Nom de domaine (VULNITLAB)
- Comptes administrateur local (\*unknown\*\\*unknown\* (8), SQL2K\ToBeFound (1))

ainsi que d'autres informations utiles sur les droits des comptes énumérés, politiques de sécurité, imprimantes, etc.

### Configuration / Service Discard

Critique

**Description** : Le service Discard est activé sur ce serveur. Ce service est inutilisé de nos jours et devrait être coupé.

**Résolution** : Désactiver le service Discard, via /etc/inetd.conf sur Unix, ou via la clé de



registre "EnableTcpDiscard" sur Windows.

**Priorité** : Critique

**Méthodologie** : boîte noire

**Risque** : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

### Configuration / Communauté SNMP publique

Critique

**Description** : Un service SNMP en version 1 ou 2 (sans mot de passe) et avec un nom de communauté commun (cf. ci-dessous) est accessible et fournit de nombreuses informations précieuses sur le système.

**Résolution** : Migrer vers SNMP v3 pour ajouter une authentification. A défaut, changer le nom de la communauté ou restreindre les machines habilitées à accéder au service SNMP.

**Priorité** : Critique

**Méthodologie** : boîte noire

**Risque** : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

**Informations** : Communautés [public, private].

Voici un échantillon d'informations utiles pouvant être collectées par SNMP :

- Matériel et logiciel (Hardware: x86 Family 6 Model 10 Stepping 7 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free))
- Nom de la machine (SQL2K)
- Comptes utilisateur (Guest, ToBeFound, Administrator, IUSR\_VULNITSMB, IWAM\_VULNITSMB, TsInternetUser)
- Interfaces réseau (127.0.0.1 / 255.0.0.0, 192.168.1.45 / 255.255.255.0)
- Programmes installés (Microsoft SQL Server 2000 (SQL2KVINCENT), WebFldrs)
- Connexions IIS actives (0)
- Partages réseau (TESTSMB, pourtous)
- Emplacement (Paris)
- Contact (vmaury@vulnit.com)

ainsi que d'autres informations utiles comme les processus, le stockage, les tables de routage, connexions TCP et UDP, etc.

### Contrôle d'accès / Relai mail ouvert

Élevé

**Description** : Ce service mail ne contrôle pas l'adresse émetteur, ce qui pourrait permettre l'usurpation d'identité. De plus, ce serveur mail (SMTP) peut servir de relai à n'importe quel émetteur, et en particulier pour relayer des spams.

**Résolution** : Appliquer les patches correctifs. Configurer le serveur pour contrôle l'émetteur du message.

**Priorité** : Élevé

**Méthodologie** : boîte noire

**Risque** : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:C/A:N/).

**Informations** : L'envoi de mails dont l'identité est usurpée semble possible. Toutefois, seul l'envoi effectif de mail (en précisant une adresse destinataire) peut permettre de valider cette vulnérabilité.

**Patch mgt / Application des correctifs Web****Élevé**

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Élevé

**Méthodologie :** boîte noire

- Résumé : IIS XSS via 404 error  
Script de test et informations relatives à cette vulnérabilité : [10936](#)  
Risque : 7.6 (Impact : 6.6, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P).  
Références : [CVE-2002-0150](#) , [CVE-2002-0148](#)



## VULNITLAB\SQL2K5 (192.168.1.54)

### Patch mgt / Application des correctifs Windows

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte blanche

- Correctif manquant : MS11-042  
Résumé : Microsoft Distributed File System Remote Code Execution Vulnerabilities (2535512)  
Script de test et informations relatives à cette vulnérabilité : 900288  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-1868 , CVE-2011-1869
- Correctif manquant : MS09-037  
Résumé : Vulnerabilities in Microsoft ATL Could Allow Remote Code Execution (973908)  
Script de test et informations relatives à cette vulnérabilité : 101100  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2009-0901 , CVE-2009-2494 , CVE-2009-2493 , CVE-2008-0015
- Correctif manquant : MS08-076  
Résumé : Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)  
Script de test et informations relatives à cette vulnérabilité : 900060  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2008-3010 , CVE-2008-3009
- Correctif manquant : MS11-020  
Résumé : Microsoft Windows SMB Server Remote Code Execution Vulnerability (2508429)  
Script de test et informations relatives à cette vulnérabilité : 900280  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0661
- Correctif manquant : MS10-020  
Résumé : Microsoft SMB Client Remote Code Execution Vulnerabilities (980232)  
Script de test et informations relatives à cette vulnérabilité : 902156  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-0476 , CVE-2010-0269 , CVE-2010-0270 , CVE-2010-0477 , CVE-2009-3676
- Correctif manquant : MS09-071  
Résumé : Microsoft Windows IAS Remote Code Execution Vulnerability (974318)  
Script de test et informations relatives à cette vulnérabilité : 901065  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2009-2505 , CVE-2009-3677
- Résumé : Microsoft Windows 2k3 Active Directory 'BROWSER ELECTION' Buffer Overflow Vulnerability  
Script de test et informations relatives à cette vulnérabilité : 801598  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0654
- Correctif manquant : MS03-039  
Résumé : Microsoft RPC Interface Buffer Overrun (KB824146)  
Script de test et informations relatives à cette vulnérabilité : 102015  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2003-0715 , CVE-2003-0528 , CVE-2003-0605
- Correctif manquant : ms08-007  
Résumé : Mini-Redirector Heap Overflow Vulnerability  
Script de test et informations relatives à cette vulnérabilité : 90015  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2008-0080
- Correctif manquant : MS11-019  
Résumé : Microsoft SMB Client Remote Code Execution Vulnerabilities (2511455)  
Script de test et informations relatives à cette vulnérabilité : 900279  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0660 , CVE-2011-0654



- Correctif manquant : [MS11-043](#)  
Résumé : Microsoft SMB Client Remote Code Execution Vulnerabilities (2536276)  
Script de test et informations relatives à cette vulnérabilité : [900287](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2011-1268](#)
- Correctif manquant : [MS08-067](#)  
Résumé : Server Service Could Allow Remote Code Execution Vulnerability (958644)  
Script de test et informations relatives à cette vulnérabilité : [900055](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-4250](#)
- Correctif manquant : [MS08-063](#)  
Résumé : SMB Remote Code Execution Vulnerability (957095)  
Script de test et informations relatives à cette vulnérabilité : [900053](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-4038](#)
- Correctif manquant : [MS10-054](#)  
Résumé : Microsoft Windows SMB Code Execution and DoS Vulnerabilities (982214)  
Script de test et informations relatives à cette vulnérabilité : [901140](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-2550](#) , [CVE-2010-2552](#) , [CVE-2010-2551](#)
- Correctif manquant : [MS09-001](#)  
Résumé : Vulnerabilities in SMB Could Allow Remote Code Execution (958687)  
Script de test et informations relatives à cette vulnérabilité : [900069](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-4835](#) , [CVE-2008-4114](#) , [CVE-2008-4834](#)
- Correctif manquant : [MS10-012](#)  
Résumé : Microsoft Windows SMB Server Multiple Vulnerabilities (971468)  
Script de test et informations relatives à cette vulnérabilité : [900230](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
- Correctif manquant : [MS09-022](#)  
Résumé : Vulnerabilities in Print Spooler Could Allow Remote Code Execution (961501)  
Script de test et informations relatives à cette vulnérabilité : [900667](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-0228](#) , [CVE-2009-0230](#) , [CVE-2009-0229](#)
- Correctif manquant : [MS09-026](#)  
Résumé : Vulnerability in RPC Could Allow Elevation of Privilege (970238)  
Script de test et informations relatives à cette vulnérabilité : [900668](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-0568](#)
- Correctif manquant : [MS10-012](#)  
Résumé : Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)  
Script de test et informations relatives à cette vulnérabilité : [902269](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
- Correctif manquant : [MS09-034](#)  
Résumé : Cumulative Security Update for Internet Explorer (972260)  
Script de test et informations relatives à cette vulnérabilité : [900906](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-1918](#) , [CVE-2009-1919](#) , [CVE-2009-1917](#)
- Correctif manquant : [MS09-042](#)  
Résumé : Telnet NTLM Credential Reflection Authentication Bypass Vulnerability (960859)  
Script de test et informations relatives à cette vulnérabilité : [900909](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-1930](#)
- Résumé : SMB Registry : Windows Service Pack version  
Script de test et informations relatives à cette vulnérabilité : [10401](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-1999-0662](#)
- Correctif manquant : [MS08-037](#)  
Résumé : Vulnerabilities in DNS Could Allow Spoofing (953230)  
Script de test et informations relatives à cette vulnérabilité : [900005](#)  
Risque : 9.4 (Impact : 9.2, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:N/I:C/A:C/\)](#).  
Références : [CVE-2008-1454](#) , [CVE-2008-1447](#)
- Correctif manquant : [MS09-029](#)  
Résumé : Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerabilities (961371))  
Script de test et informations relatives à cette vulnérabilité : [900689](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).



- Références : [CVE-2009-0231](#) , [CVE-2009-0232](#)
- Correctif manquant : [MS10-001](#)  
Résumé : Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerabilities (972270)  
Script de test et informations relatives à cette vulnérabilité : [901095](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0018](#)
  - Correctif manquant : [MS10-082](#)  
Résumé : Microsoft Windows Media Player Remote Code Execution Vulnerability (2378111)  
Script de test et informations relatives à cette vulnérabilité : [901163](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-2745](#)
  - Correctif manquant : [MS10-035](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (982381)  
Script de test et informations relatives à cette vulnérabilité : [902191](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-1261](#) , [CVE-2010-1259](#) , [CVE-2010-0255](#) , [CVE-2010-1262](#) , [CVE-2010-1260](#) , [CVE-2010-1257](#)
  - Correctif manquant : [MS07-042](#)  
Résumé : Microsoft XML Core Services Remote Code Execution Vulnerability (936227)  
Script de test et informations relatives à cette vulnérabilité : [801715](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2007-2223](#)
  - Correctif manquant : [MS10-090](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2416400)  
Script de test et informations relatives à cette vulnérabilité : [900262](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-3340](#) , [CVE-2010-3962](#) , [CVE-2010-3346](#) , [CVE-2010-3343](#) , [CVE-2010-3345](#) , [CVE-2010-3348](#) , [CVE-2010-3342](#)
  - Correctif manquant : [MS08-024](#)  
Résumé : Microsoft Internet Explorer Data Stream Handling Remote Code Execution Vulnerability (947864)  
Script de test et informations relatives à cette vulnérabilité : [801488](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-1085](#)
  - Correctif manquant : [MS08-069](#)  
Résumé : Microsoft XML Core Services Remote Code Execution Vulnerability (955218)  
Script de test et informations relatives à cette vulnérabilité : [900058](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-4033](#) , [CVE-2008-4029](#) , [CVE-2007-0099](#)
  - Correctif manquant : [MS10-053](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2183461)  
Script de test et informations relatives à cette vulnérabilité : [901139](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-2557](#) , [CVE-2010-2558](#) , [CVE-2010-2560](#) , [CVE-2010-1258](#) , [CVE-2010-2556](#) , [CVE-2010-2559](#)
  - Correctif manquant : [MS11-003](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2482017)  
Script de test et informations relatives à cette vulnérabilité : [901180](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2011-0035](#) , [CVE-2011-0038](#) , [CVE-2011-0036](#) , [CVE-2010-3971](#)
  - Correctif manquant : [MS08-001](#)  
Résumé : Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (941644)  
Script de test et informations relatives à cette vulnérabilité : [801706](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2007-0069](#) , [CVE-2007-0066](#)
  - Correctif manquant : [MS10-062](#)  
Résumé : MPEG-4 Codec Remote Code Execution Vulnerability (975558)  
Script de test et informations relatives à cette vulnérabilité : [900250](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0818](#)
  - Correctif manquant : [MS07-050](#)  
Résumé : Microsoft Windows Vector Markup Language Buffer Overflow (938127)  
Script de test et informations relatives à cette vulnérabilité : [102059](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2007-1749](#)
  - Correctif manquant : [MS09-011](#)  
Résumé : Microsoft DirectShow Remote Code Execution Vulnerability (961373)  
Script de test et informations relatives à cette vulnérabilité : [900093](#)



- Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-0084
- Correctif manquant : MS08-010  
 Résumé : Microsoft Internet Explorer HTML Rendering Remote Memory Corruption Vulnerability (944533)  
 Script de test et informations relatives à cette vulnérabilité : 801702  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2008-0076
- Correctif manquant : MS10-005  
 Résumé : Microsoft Paint Remote Code Execution Vulnerability (978706)  
 Script de test et informations relatives à cette vulnérabilité : 902015  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2010-0028
- Correctif manquant : MS10-013  
 Résumé : Microsoft DirectShow Remote Code Execution Vulnerability (977935)  
 Script de test et informations relatives à cette vulnérabilité : 902117  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2010-0250
- Correctif manquant : MS09-046  
 Résumé : Microsoft DHTML Editing Component ActiveX Remote Code Execution Vulnerability (956844)  
 Script de test et informations relatives à cette vulnérabilité : 900837  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-2519
- Correctif manquant : MS10-042  
 Résumé : Microsoft Help and Support Center Remote Code Execution Vulnerability (2229593)  
 Script de test et informations relatives à cette vulnérabilité : 902080  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2010-1885
- Correctif manquant : MS10-007  
 Résumé : Microsoft Windows Shell Handler Could Allow Remote Code Execution Vulnerability (975713)  
 Script de test et informations relatives à cette vulnérabilité : 900227  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2010-0027
- Correctif manquant : MS09-052  
 Résumé : Microsoft Windows Media Player ASF Heap Overflow Vulnerability (974112)  
 Script de test et informations relatives à cette vulnérabilité : 900879  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-2527
- Correctif manquant : MS09-057  
 Résumé : Microsoft Windows Indexing Service ActiveX Vulnerability (969059)  
 Script de test et informations relatives à cette vulnérabilité : 900881  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-2507
- Correctif manquant : MS10-091  
 Résumé : Microsoft Windows OpenType Compact Font Format Driver Privilege Escalation Vulnerability (2296199)  
 Script de test et informations relatives à cette vulnérabilité : 900263  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2010-3957 , CVE-2010-3956 , CVE-2010-3959
- Correctif manquant : MS09-047  
 Résumé : sMicrosoft Windows Media Format Remote Code Execution Vulnerability (973812)  
 Script de test et informations relatives à cette vulnérabilité : 901012  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-2499 , CVE-2009-2498
- Correctif manquant : MS09-061  
 Résumé : Microsoft .NET Common Language Runtime Code Execution Vulnerability (974378)  
 Script de test et informations relatives à cette vulnérabilité : 900964  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2009-2497 , CVE-2009-0091 , CVE-2009-0090
- Correctif manquant : MS07-064  
 Résumé : Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)  
 Script de test et informations relatives à cette vulnérabilité : 801710  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : CVE-2007-3895 , CVE-2007-3901
- Résumé : Microsoft Video ActiveX Control 'msvidctl.dll' BOF Vulnerability



- Script de test et informations relatives à cette vulnérabilité : [800829](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-0020](#) , [CVE-2008-0015](#)
- Correctif manquant : [MS10-018](#)  
 Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (980182)  
 Script de test et informations relatives à cette vulnérabilité : [902155](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0267](#) , [CVE-2010-0492](#) , [CVE-2010-0490](#) , [CVE-2010-0807](#) , [CVE-2010-0489](#) , [CVE-2010-0491](#) , [CVE-2010-0805](#) , [CVE-2010-0806](#) , [CVE-2010-0488](#) , [CVE-2010-0494](#)
  - Correctif manquant : [MS11-038](#)  
 Résumé : Microsoft Windows OLE Automation Remote Code Execution Vulnerability (2476490)  
 Script de test et informations relatives à cette vulnérabilité : [902377](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-0658](#)
  - Packet affecté : -INTERNET EXPLORER  
 Résumé : Microsoft Internet Explorer HTML Form Value DoS Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [900303](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2009-0341](#)
  - Correctif manquant : [MS07-045](#)  
 Résumé : Cumulative Security Update for Internet Explorer (937143)  
 Script de test et informations relatives à cette vulnérabilité : [102058](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2007-3041](#) , [CVE-2007-0943](#) , [CVE-2007-2216](#)
  - Correctif manquant : [MS09-045](#)  
 Résumé : Microsoft JScript Scripting Engine Remote Code Execution Vulnerability (971961)  
 Script de test et informations relatives à cette vulnérabilité : [900929](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2009-1920](#)
  - Correctif manquant : [MS10-002](#)  
 Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (978207)  
 Script de test et informations relatives à cette vulnérabilité : [901097](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0027](#) , [CVE-2009-4074](#) , [CVE-2010-0245](#) , [CVE-2010-0246](#) , [CVE-2010-0249](#) , [CVE-2010-0247](#) , [CVE-2010-0244](#) , [CVE-2010-0248](#)
  - Correctif manquant : [MS10-030](#)  
 Résumé : Microsoft Outlook Express and Windows Mail Remote Code Execution Vulnerability (978542)  
 Script de test et informations relatives à cette vulnérabilité : [900241](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0816](#)
  - Packet affecté : -WINDOWS MEDIA PLAYER  
 Résumé : Microsoft Windows Media Player MID File Integer Overflow Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [900336](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2009-1331](#)
  - Correctif manquant : [MS09-065](#)  
 Résumé : Microsoft Windows Kernel-Mode Drivers Multiple Vulnerabilities (969947)  
 Script de test et informations relatives à cette vulnérabilité : [900886](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2009-2514](#) , [CVE-2009-2513](#) , [CVE-2009-1127](#)
  - Correctif manquant : [MS07-068](#)  
 Résumé : Vulnerability in Windows Media File Format Could Allow Remote Code Execution  
 Script de test et informations relatives à cette vulnérabilité : [801708](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2007-0064](#)
  - Correctif manquant : [MS10-096](#)  
 Résumé : Microsoft Windows Address Book Remote Code Execution Vulnerability (2423089)  
 Script de test et informations relatives à cette vulnérabilité : [901169](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-3147](#)
  - Correctif manquant : [MS08-046](#)  
 Résumé : Microsoft Windows Image Color Management System Code Execution Vulnerability (952954)  
 Script de test et informations relatives à cette vulnérabilité : [800023](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-2245](#)



- Correctif manquant : [MS07-027](#)  
Résumé : Cumulative Security Update for Internet Explorer (931768)  
Script de test et informations relatives à cette vulnérabilité : [102056](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-0944](#) , [CVE-2007-0945](#) , [CVE-2007-2221](#) , [CVE-2007-0942](#) , [CVE-2007-0947](#)
- Correctif manquant : [MS07-056](#)  
Résumé : Microsoft Outlook Express And Windows Mail NNTP Protocol Heap Buffer Overflow Vulnerability (941202)  
Script de test et informations relatives à cette vulnérabilité : [801713](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-3897](#)
- Correctif manquant : [MS10-052](#)  
Résumé : Microsoft Window MPEG Layer-3 Remote Code Execution Vulnerability (2115168)  
Script de test et informations relatives à cette vulnérabilité : [902229](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-1882](#)
- Correctif manquant : [MS10-061](#)  
Résumé : Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability(2347290)  
Script de test et informations relatives à cette vulnérabilité : [901150](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-2729](#)
- Correctif manquant : [MS10-006](#)  
Résumé : Microsoft SMB Client Remote Code Execution Vulnerabilities (978251)  
Script de test et informations relatives à cette vulnérabilité : [902112](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-0016](#) , [CVE-2010-0017](#)
- Correctif manquant : [MS08-071](#)  
Résumé : Vulnerabilities in GDI Could Allow Remote Code Execution (956802)  
Script de test et informations relatives à cette vulnérabilité : [900059](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2008-2249](#) , [CVE-2008-3465](#)
- Correctif manquant : [MS09-028](#)  
Résumé : Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution  
Script de test et informations relatives à cette vulnérabilité : [900097](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-1537](#)
- Correctif manquant : [MS11-071](#)  
Résumé : Microsoft Windows Components Remote Code Execution Vulnerabilities (2570947)  
Script de test et informations relatives à cette vulnérabilité : [901205](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-1991](#)
- Correctif manquant : [MS11-018](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2497640)  
Script de test et informations relatives à cette vulnérabilité : [900278](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-1245](#) , [CVE-2011-1345](#) , [CVE-2011-0346](#) , [CVE-2011-0094](#) , [CVE-2011-1244](#)
- Correctif manquant : [MS07-033](#)  
Résumé : Cumulative Security Update for Internet Explorer (933566)  
Script de test et informations relatives à cette vulnérabilité : [102057](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-1751](#) , [CVE-2007-1750](#) , [CVE-2007-2222](#) , [CVE-2007-3027](#) , [CVE-2007-0218](#) , [CVE-2007-1499](#)
- Résumé : .NET JIT Compiler Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [90010](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-0043](#)
- Correctif manquant : [MS11-007](#)  
Résumé : Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)  
Script de test et informations relatives à cette vulnérabilité : [902335](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-0033](#)
- Correctif manquant : [MS10-097](#)  
Résumé : MS Windows ICSW Remote Code Execution Vulnerability (2443105)  
Script de test et informations relatives à cette vulnérabilité : [902278](#)



- Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-3144](#)
- Correctif manquant : [MS11-032](#)  
Résumé : Windows OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (2507618)  
Script de test et informations relatives à cette vulnérabilité : [902363](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2011-0034](#)
  - Correctif manquant : [MS09-015](#)  
Résumé : Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)  
Script de test et informations relatives à cette vulnérabilité : [900533](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-2540](#)
  - Correctif manquant : [MS08-073](#)  
Résumé : Cumulative Security Update for Internet Explorer (958215)  
Script de test et informations relatives à cette vulnérabilité : [900062](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-4258](#) , [CVE-2008-4259](#) , [CVE-2008-4260](#) , [CVE-2008-4261](#)
  - Correctif manquant : [MS08-038](#)  
Résumé : Microsoft Autorun Arbitrary Code Execution Vulnerability (08-038)  
Script de test et informations relatives à cette vulnérabilité : [900445](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-0243](#) , [CVE-2008-0951](#)
  - Correctif manquant : [MS09-055](#)  
Résumé : Microsoft Windows ATL COM Initialization Code Execution Vulnerability (973525)  
Script de test et informations relatives à cette vulnérabilité : [900880](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-2493](#)
  - Correctif manquant : [MS11-031](#)  
Résumé : Microsoft JScript and VBScript Scripting Engines Remote Code Execution Vulnerability (2514666)  
Script de test et informations relatives à cette vulnérabilité : [902501](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2011-0663](#)
  - Packet affecté : -INTERNET EXPLORER  
Résumé : Microsoft Internet Explorer Remote Code Execution Vulnerability (979352)  
Script de test et informations relatives à cette vulnérabilité : [800429](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0249](#)
  - Correctif manquant : [MS07-057](#)  
Résumé : Cumulative Security Update for Internet Explorer (939653)  
Script de test et informations relatives à cette vulnérabilité : [102060](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2007-3893](#) , [CVE-2007-3892](#) , [CVE-2007-3826](#)
  - Correctif manquant : [MS10-076](#)  
Résumé : Embedded OpenType Font Engine Remote Code Execution Vulnerability (982132)  
Script de test et informations relatives à cette vulnérabilité : [902321](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-1883](#)
  - Correctif manquant : [MS08-033](#)  
Résumé : Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)  
Script de test et informations relatives à cette vulnérabilité : [800104](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2008-0011](#) , [CVE-2008-1444](#)
  - Correctif manquant : [MS10-074](#)  
Résumé : Microsoft Foundation Classes Could Allow Remote Code Execution Vulnerability (2387149)  
Script de test et informations relatives à cette vulnérabilité : [902319](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-3227](#)
  - Correctif manquant : [MS10-051](#)  
Résumé : Microsoft Windows LSASS Denial of Service Vulnerability (975467)  
Script de test et informations relatives à cette vulnérabilité : [902227](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-2561](#)
  - Correctif manquant : [MS10-066](#)  
Résumé : Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802)



- Script de test et informations relatives à cette vulnérabilité : [902300](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-2567](#)
- Correctif manquant : [MS09-054](#)  
Résumé : Microsoft Internet Explorer Multiple Code Execution Vulnerabilities (974455)  
Script de test et informations relatives à cette vulnérabilité : [901041](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-2530](#), [CVE-2009-1547](#), [CVE-2009-2529](#), [CVE-2009-2531](#)
  - Correctif manquant : [954157](#)  
Résumé : Microsoft Windows Indeo Codec Multiple Vulnerabilities  
Script de test et informations relatives à cette vulnérabilité : [801090](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-4313](#), [CVE-2009-4309](#), [CVE-2009-4310](#), [CVE-2009-4210](#), [CVE-2009-4312](#), [CVE-2009-4311](#)
  - Correctif manquant : [MS11-029](#)  
Résumé : Microsoft GDI+ Remote Code Execution Vulnerability (2489979)  
Script de test et informations relatives à cette vulnérabilité : [902365](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-0041](#)
  - Correctif manquant : [MS09-014](#)  
Résumé : Microsoft Internet Explorer Remote Code Execution Vulnerability (963027)  
Script de test et informations relatives à cette vulnérabilité : [900328](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-0554](#), [CVE-2009-0553](#), [CVE-2009-0550](#), [CVE-2009-0552](#), [CVE-2008-2540](#), [CVE-2009-0551](#)
  - Correctif manquant : [MS11-006](#)  
Résumé : Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)  
Script de test et informations relatives à cette vulnérabilité : [902334](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3970](#)
  - Correctif manquant : [MS07-017](#)  
Résumé : Vulnerabilities in GDI Could Allow Remote Code Execution (925902)  
Script de test et informations relatives à cette vulnérabilité : [801720](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-1215](#), [CVE-2007-1211](#), [CVE-2007-0038](#), [CVE-2007-1213](#), [CVE-2007-1212](#)
  - Correctif manquant : [MS08-045](#)  
Résumé : Cumulative Security Update for Internet Explorer (953838)  
Script de test et informations relatives à cette vulnérabilité : [900030](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2008-2257](#), [CVE-2008-2258](#), [CVE-2008-2254](#), [CVE-2008-2259](#), [CVE-2008-2256](#), [CVE-2008-2255](#)
  - Correctif manquant : [MS08-068](#)  
Résumé : SMB Could Allow Remote Code Execution Vulnerability (957097)  
Script de test et informations relatives à cette vulnérabilité : [900057](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2008-4037](#)
  - Correctif manquant : [MS10-071](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2360131)  
Script de test et informations relatives à cette vulnérabilité : [901162](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3325](#), [CVE-2010-3329](#), [CVE-2010-3328](#), [CVE-2010-3330](#), [CVE-2010-3331](#), [CVE-2010-3326](#), [CVE-2010-3327](#), [CVE-2010-3243](#), [CVE-2010-0808](#), [CVE-2010-3324](#)
  - Correctif manquant : [MS09-006](#)  
Résumé : Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)  
Script de test et informations relatives à cette vulnérabilité : [900086](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-0082](#), [CVE-2009-0083](#), [CVE-2009-0081](#)
  - Correctif manquant : [MS10-046](#)  
Résumé : Microsoft Windows Shell Remote Code Execution Vulnerability (2286198)  
Script de test et informations relatives à cette vulnérabilité : [902226](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-2568](#)
  - Correctif manquant : [MS08-058](#)  
Résumé : Cumulative Security Update for Internet Explorer (956390)  
Script de test et informations relatives à cette vulnérabilité : [900054](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).



- Références : [CVE-2008-3474](#) , [CVE-2008-3476](#) , [CVE-2008-3473](#) , [CVE-2008-3475](#) , [CVE-2008-3472](#) , [CVE-2008-2947](#)
- Correctif manquant : [MS07-034](#)  
Résumé : Microsoft Outlook Express/Windows Mail MHTML URI Handler Information Disclosure Vulnerability (929123)  
Script de test et informations relatives à cette vulnérabilité : [801716](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2006-2111](#) , [CVE-2007-2225](#) , [CVE-2007-2225](#) , [CVE-2007-1658](#)
  - Correctif manquant : [MS11-050](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2530548)  
Script de test et informations relatives à cette vulnérabilité : [902443](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-1251](#) , [CVE-2011-1256](#) , [CVE-2011-1250](#) , [CVE-2011-1254](#) , [CVE-2011-1246](#) , [CVE-2011-1255](#) , [CVE-2011-1252](#) , [CVE-2011-1261](#) , [CVE-2011-1258](#) , [CVE-2011-1262](#) , [CVE-2011-1260](#)
  - Correctif manquant : [MS11-057](#)  
Résumé : Microsoft Internet Explorer Multiple Vulnerabilities (2559049)  
Script de test et informations relatives à cette vulnérabilité : [902613](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2011-1257](#) , [CVE-2011-1962](#) , [CVE-2011-1963](#) , [CVE-2011-1960](#) , [CVE-2011-1961](#) , [CVE-2011-1964](#) , [CVE-2011-2383](#)
  - Résumé : MS Internet Explorer 'Style' Object Remote Code Execution Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [800727](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-3674](#) , [CVE-2009-3671](#) , [CVE-2009-3673](#) , [CVE-2009-3672](#) , [CVE-2009-2493](#)
  - Correctif manquant : [MS09-051](#)  
Résumé : Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)  
Script de test et informations relatives à cette vulnérabilité : [901039](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-2525](#) , [CVE-2009-0555](#)
  - Correctif manquant : [MS07-004](#)  
Résumé : Microsoft Windows Vector Markup Language Vulnerabilities (929969)  
Script de test et informations relatives à cette vulnérabilité : [102053](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-0024](#)
  - Correctif manquant : [MS09-038](#)  
Résumé : Microsoft Windows AVI Media File Parsing Vulnerabilities (971557)  
Script de test et informations relatives à cette vulnérabilité : [900907](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2009-1545](#) , [CVE-2009-1546](#)
  - Correctif manquant : [ms08-028](#)  
Résumé : Windows Vulnerability in Microsoft Jet Database Engine  
Script de test et informations relatives à cette vulnérabilité : [90024](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-6026](#)
  - Correctif manquant : [ms08-078](#)  
Résumé : Vulnerability in Internet Explorer Could Allow Remote Code Execution (960714)  
Script de test et informations relatives à cette vulnérabilité : [900066](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2008-4844](#)
  - Correctif manquant : [MS09-019](#)  
Résumé : Cumulative Security Update for Internet Explorer (969897)  
Script de test et informations relatives à cette vulnérabilité : [900364](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-3091](#) , [CVE-2009-1528](#) , [CVE-2009-1529](#) , [CVE-2009-1531](#) , [CVE-2009-1140](#) , [CVE-2009-1532](#) , [CVE-2009-1530](#) , [CVE-2009-1141](#)
  - Correctif manquant : [MS07-069](#)  
Résumé : Microsoft Internet Explorer mshtml.dll Remote Memory Corruption Vulnerability (942615)  
Script de test et informations relatives à cette vulnérabilité : [801707](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2007-5344](#) , [CVE-2007-3903](#) , [CVE-2007-3902](#) , [CVE-2007-5347](#)
  - Résumé : Microsoft Windows Progman Group Converter Insecure Library Loading Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [801456](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
Références : [CVE-2010-3139](#)



- Correctif manquant : [MS08-031](#)  
Résumé : Cumulative Security Update for Internet Explorer (950759)  
Script de test et informations relatives à cette vulnérabilité : [800103](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2008-1442](#) , [CVE-2008-1544](#)
- Packet affecté : -INTERNET EXPLORER  
Résumé : MS Internet Explorer Remote Code Execution Vulnerability (981374)  
Script de test et informations relatives à cette vulnérabilité : [800176](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2010-0806](#)
- Correctif manquant : [MS08-049](#)  
Résumé : Vulnerabilities in Event System Could Allow Remote Code Execution (950974)  
Script de test et informations relatives à cette vulnérabilité : [900035](#)  
Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : [\(AV:N/AC:L/AU:S/C:C/I:C/A/C/\)](#).  
Références : [CVE-2008-1456](#) , [CVE-2008-1457](#)
- Correctif manquant : [MS09-012](#)  
Résumé : Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)  
Script de test et informations relatives à cette vulnérabilité : [900094](#)  
Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : [\(AV:N/AC:L/AU:S/C:C/I:C/A/C/\)](#).  
Références : [CVE-2009-0078](#) , [CVE-2009-0080](#) , [CVE-2009-0079](#) , [CVE-2008-1436](#)
- Correctif manquant : [MS08-062](#)  
Résumé : Windows Internet Printing Service Allow Remote Code Execution Vulnerability (953155)  
Script de test et informations relatives à cette vulnérabilité : [900052](#)  
Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : [\(AV:N/AC:L/AU:S/C:C/I:C/A/C/\)](#).  
Références : [CVE-2008-1446](#)
- Correctif manquant : [MS08-020](#)  
Résumé : Microsoft Windows DNS Client Service Response Spoofing Vulnerability (945553)  
Script de test et informations relatives à cette vulnérabilité : [801701](#)  
Risque : 8.8 (Impact : 9.2, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:N/I:C/A/C/\)](#).  
Références : [CVE-2008-0087](#)
- Correctif manquant : [ms08-020](#)  
Résumé : Windows vulnerability in DNS Client Could Allow Spoofing (945553)  
Script de test et informations relatives à cette vulnérabilité : [90020](#)  
Risque : 8.8 (Impact : 9.2, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:N/I:C/A/C/\)](#).  
Références : [CVE-2008-0087](#)
- Correctif manquant : [MS10-040](#)  
Résumé : Microsoft IIS Authentication Remote Code Execution Vulnerability (982666)  
Script de test et informations relatives à cette vulnérabilité : [901120](#)  
Risque : 8.5 (Impact : 10.0, Exploitabilité : 6.8) CVSS : [\(AV:N/AC:M/AU:S/C:C/I:C/A/C/\)](#).  
Références : [CVE-2010-1256](#)
- Correctif manquant : [MS07-058](#)  
Résumé : Vulnerability in RPC Could Allow Denial of Service (933729)  
Script de test et informations relatives à cette vulnérabilité : [801712](#)  
Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:N/I:N/A/C/\)](#).  
Références : [CVE-2007-2228](#)
- Correctif manquant : [981169](#)  
Résumé : MS Internet Explorer 'VBScript' Remote Code Execution Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [800482](#)  
Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2010-0483](#)
- Correctif manquant : [MS08-032](#)  
Résumé : Microsoft Windows Speech Components Voice Recognition Command Execution Vulnerability (950760)  
Script de test et informations relatives à cette vulnérabilité : [801486](#)  
Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2007-0675](#)
- Correctif manquant : [MS11-024](#)  
Résumé : Windows Fax Cover Page Editor Remote Code Execution Vulnerability (2527308)  
Script de test et informations relatives à cette vulnérabilité : [902408](#)  
Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2010-3974](#)
- Correctif manquant : [MS07-047](#)  
Résumé : Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782)  
Script de test et informations relatives à cette vulnérabilité : [801714](#)  
Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A/C/\)](#).  
Références : [CVE-2007-3035](#) , [CVE-2007-3037](#)
- Correctif manquant : [MS10-081](#)



- Résumé : Windows Common Control Library Remote Code Execution Vulnerability (2296011)  
 Script de test et informations relatives à cette vulnérabilité : [901165](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2010-2746](#)
- Correctif manquant : [MS10-022](#)  
 Résumé : Microsoft VBScript Scripting Engine Remote Code Execution Vulnerability (980232)  
 Script de test et informations relatives à cette vulnérabilité : [902159](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : [\(AV:N/AC:H/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2010-0483](#)
- Résumé : Microsoft RPC Interface Buffer Overrun (823980)  
 Script de test et informations relatives à cette vulnérabilité : [11808](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:P/I:P/A:P/\)](#).  
 Références : [CVE-2003-0352](#)
- Correctif manquant : [MS09-056](#)  
 Résumé : Microsoft Windows CryptoAPI X.509 Spoofing Vulnerabilities (974571)  
 Script de test et informations relatives à cette vulnérabilité : [900876](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:P/I:P/A:P/\)](#).  
 Références : [CVE-2009-2510](#) , [CVE-2009-2511](#)
- Correctif manquant : [MS11-030](#)  
 Résumé : Microsoft DNS Resolution Remote Code Execution Vulnerability (2509553)  
 Script de test et informations relatives à cette vulnérabilité : [900282](#)  
 Risque : 7.5 (Impact : 6.4, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:P/I:P/A:P/\)](#).  
 Références : [CVE-2011-0657](#)
- Correctif manquant : [MS10-037](#)  
 Résumé : Microsoft Windows OpenType Compact Font Format Driver Privilege Escalation Vulnerability (980218)  
 Script de test et informations relatives à cette vulnérabilité : [901119](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2010-0819](#)
- Correctif manquant : [MS10-099](#)  
 Résumé : Routing and Remote Access Privilege Escalation Vulnerability (2440591)  
 Script de test et informations relatives à cette vulnérabilité : [900264](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2010-3963](#)
- Correctif manquant : [MS11-063](#)  
 Résumé : Microsoft Windows Client/Server Run-time Subsystem Privilege Escalation Vulnerability (2567680)  
 Script de test et informations relatives à cette vulnérabilité : [902463](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2011-1967](#)
- Correctif manquant : [MS09-058](#)  
 Résumé : Microsoft Windows Kernel Privilege Escalation Vulnerability (971486)  
 Script de test et informations relatives à cette vulnérabilité : [900963](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2009-2517](#) , [CVE-2009-2516](#) , [CVE-2009-2515](#)
- Correctif manquant : [MS08-036](#)  
 Résumé : Microsoft Pragmatic General Multicast (PGM) Denial of Service Vulnerability (950762)  
 Script de test et informations relatives à cette vulnérabilité : [801485](#)  
 Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:N/I:N/A:C/\)](#).  
 Références : [CVE-2008-1441](#) , [CVE-2008-1440](#)
- Correctif manquant : [MS08-048](#)  
 Résumé : Security Update for Outlook Express (951066)  
 Script de test et informations relatives à cette vulnérabilité : [900031](#)  
 Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:N/A:N/\)](#).  
 Références : [CVE-2008-1448](#)
- Correctif manquant : [MS10-098](#)  
 Résumé : Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2436673)  
 Script de test et informations relatives à cette vulnérabilité : [902275](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2010-3941](#) , [CVE-2010-3942](#) , [CVE-2010-3940](#) , [CVE-2010-3939](#) , [CVE-2010-3943](#)
- Correctif manquant : [MS08-066](#)  
 Résumé : Microsoft Ancillary Function Driver Elevation of Privilege Vulnerability (956803)  
 Script de test et informations relatives à cette vulnérabilité : [900223](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : [\(AV:L/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
 Références : [CVE-2008-3464](#)
- Packet affecté : -INTERNET EXPLORER



- Résumé : Microsoft Internet Explorer Denial Of Service Vulnerability - July09  
 Script de test et informations relatives à cette vulnérabilité : [800669](#)  
 Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2009-2536](#) , [CVE-2009-1692](#)
- Correctif manquant : [MS08-061](#)  
 Résumé : Windows Kernel Elevation of Privilege Vulnerability (954211)  
 Script de test et informations relatives à cette vulnérabilité : [900051](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-2250](#) , [CVE-2008-2251](#) , [CVE-2008-2252](#)
  - Correctif manquant : [MS08-064](#)  
 Résumé : Virtual Address Descriptor Manipulation Elevation of Privilege Vulnerability (956841)  
 Script de test et informations relatives à cette vulnérabilité : [900225](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-4036](#)
  - Résumé : Microsoft Windows Server 2003 OpenType Font Engine DoS Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [800687](#)  
 Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2009-3020](#)
  - Correctif manquant : [MS11-034](#)  
 Résumé : Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2506223)  
 Script de test et informations relatives à cette vulnérabilité : [900283](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-0676](#) , [CVE-2011-1228](#) , [CVE-2011-1231](#) , [CVE-2011-0675](#) , [CVE-2011-1226](#) , [CVE-2011-0667](#) , [CVE-2011-0677](#) , [CVE-2011-0662](#) , [CVE-2011-0674](#) , [CVE-2011-1233](#) , [CVE-2011-0670](#) , [CVE-2011-1239](#) , [CVE-2011-0671](#) , [CVE-2011-1240](#) , [CVE-2011-1229](#) , [CVE-2011-0672](#) , [CVE-2011-1234](#) , [CVE-2011-1238](#) , [CVE-2011-1227](#) , [CVE-2011-0665](#) , [CVE-2011-1232](#) , [CVE-2011-1230](#) , [CVE-2011-1241](#) , [CVE-2011-0666](#) , [CVE-2011-1237](#) , [CVE-2011-1235](#) , [CVE-2011-1225](#) , [CVE-2011-1236](#) , [CVE-2011-0673](#) , [CVE-2011-1242](#)
  - Correctif manquant : [MS11-062](#)  
 Résumé : MS Windows Remote Access Service NDISTAPI Driver Privilege Elevation Vulnerability (2566454)  
 Script de test et informations relatives à cette vulnérabilité : [900298](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-1974](#)
  - Correctif manquant : [MS11-013](#)  
 Résumé : Microsoft Kerberos Privilege Escalation Vulnerabilities (2496930)  
 Script de test et informations relatives à cette vulnérabilité : [902288](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-0043](#) , [CVE-2011-0091](#)
  - Correctif manquant : [MS11-056](#)  
 Résumé : Microsoft Windows CSRSS Privilege Escalation Vulnerabilities (2507938)  
 Script de test et informations relatives à cette vulnérabilité : [902609](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2011-1283](#) , [CVE-2011-1284](#) , [CVE-2011-1282](#) , [CVE-2011-1870](#) , [CVE-2011-1281](#)
  - Correctif manquant : [MS08-025](#)  
 Résumé : Microsoft Windows Kernel Usermode Callback Local Privilege Elevation Vulnerability (941693)  
 Script de test et informations relatives à cette vulnérabilité : [801487](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2008-1084](#)
  - Correctif manquant : [MS09-007](#)  
 Résumé : Vulnerability in SChannel Could Allow Spoofing (960225)  
 Script de test et informations relatives à cette vulnérabilité : [900087](#)  
 Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:C/A:N/).  
 Références : [CVE-2009-0085](#)
  - Correctif manquant : [MS10-084](#)  
 Résumé : Windows Local Procedure Call Privilege Elevation Vulnerability (2360937)  
 Script de test et informations relatives à cette vulnérabilité : [902322](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-3222](#)
  - Correctif manquant : [MS07-017](#)  
 Résumé : Microsoft Windows GDI Multiple Vulnerabilities (925902)  
 Script de test et informations relatives à cette vulnérabilité : [102055](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2007-1215](#) , [CVE-2006-5586](#) , [CVE-2007-1211](#) , [CVE-2006-5758](#) , [CVE-2007-1213](#) , [CVE-2007-1212](#)



- Correctif manquant : MS10-078  
Résumé : OpenType Font (OTF) Format Driver Privilege Elevation Vulnerabilities (2279986)  
Script de test et informations relatives à cette vulnérabilité : 902320  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-2740 , CVE-2010-2741
- Résumé : Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability  
Script de test et informations relatives à cette vulnérabilité : 800442  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-0232
- Correctif manquant : MS11-065  
Résumé : Microsoft Remote Desktop Protocol Denial of Service Vulnerability (2570222)  
Script de test et informations relatives à cette vulnérabilité : 902708  
Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).  
Références : CVE-2011-1968
- Correctif manquant : MS11-011  
Résumé : Microsoft Windows Kernel Elevation of Privilege Vulnerability (2393802)  
Script de test et informations relatives à cette vulnérabilité : 902337  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0045 , CVE-2010-4398
- Correctif manquant : MS09-025  
Résumé : Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)  
Script de test et informations relatives à cette vulnérabilité : 900669  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2009-1124 , CVE-2009-1125 , CVE-2009-1126 , CVE-2009-1123
- Correctif manquant : MS10-073  
Résumé : Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (981957)  
Script de test et informations relatives à cette vulnérabilité : 902323  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-2549 , CVE-2010-2743 , CVE-2010-2744
- Correctif manquant : MS11-014  
Résumé : Microsoft Windows LSASS Privilege Escalation Vulnerability (2478960)  
Script de test et informations relatives à cette vulnérabilité : 902289  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0039
- Résumé : Microsoft Windows win32k.sys Driver 'CreateDIBPalette()' BOF Vulnerability  
Script de test et informations relatives à cette vulnérabilité : 902256  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-2739
- Correctif manquant : MS11-054  
Résumé : Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2555917)  
Script de test et informations relatives à cette vulnérabilité : 902538  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-1879 , CVE-2011-1880 , CVE-2011-1884 , CVE-2011-1875 , CVE-2011-1876 , CVE-2011-1881 , CVE-2011-1882 , CVE-2011-1886 , CVE-2011-1877 , CVE-2011-1883 , CVE-2011-1887 , CVE-2011-1878 , CVE-2011-1885 , CVE-2011-1874 , CVE-2011-1888
- Correctif manquant : MS11-012  
Résumé : Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2479628)  
Script de test et informations relatives à cette vulnérabilité : 901182  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-0088 , CVE-2011-0090 , CVE-2011-0086 , CVE-2011-0089 , CVE-2011-0087
- Correctif manquant : MS10-015  
Résumé : Microsoft Windows Kernel Could Allow Elevation of Privilege (977165)  
Script de test et informations relatives à cette vulnérabilité : 900740  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2010-0232 , CVE-2010-0233
- Correctif manquant : MS11-046  
Résumé : MS Windows Ancillary Function Driver Privilege Elevation Vulnerability  
Script de test et informations relatives à cette vulnérabilité : 902442  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2011-1249
- Correctif manquant : MS07-021  
Résumé : Microsoft Windows CSRSS CSRFinalizeContext Local Privilege Escalation Vulnerability (930178)  
Script de test et informations relatives à cette vulnérabilité : 801719  
Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
Références : CVE-2007-1209 , CVE-2006-6696

**Patch mgt / Application des correctifs de bases de données****Majeur**

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Majeur

**Méthodologie :** boîte blanche

- Correctif manquant : [MS08-040](#)  
Résumé : MS SQL Server Élévation of Privilege Vulnerabilities (941203)  
Script de test et informations relatives à cette vulnérabilité : [800105](#)  
Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).  
Références : [CVE-2008-0085](#) , [CVE-2008-0086](#) , [CVE-2008-0106](#) , [CVE-2008-0107](#)

**Configuration / Liste d'instances accessible****Élevé**

**Description :** La configuration et la version du serveur Microsoft SQL permettent d'obtenir la liste des instances de bases de données.

**Résolution :** Arrêter le service 'SQL Server Browser', ou à défaut, filtrer l'accès au port 1434/UDP aux seuls clients habilités.

**Priorité :** Élevé

**Méthodologie :** boîte noire

**Risque :** 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

**Informations :** TOBEFOUND (9.00.1399.06)



## VULNITLAB\WINXP (192.168.1.84)

### Patch mgt / Application des correctifs Windows

Critique

**Description :** Les correctifs (patches) indiqués ci-dessous n'ont pas été correctement installés. Les failles de sécurité relatives n'ont donc pas été corrigées et pourraient être exploitées.

**Résolution :** Appliquer les correctifs mis à disposition par l'éditeur.

**Priorité :** Critique

**Méthodologie :** boîte blanche

- Résumé : Microsoft Windows XP SP3 denial of service vulnerability  
Script de test et informations relatives à cette vulnérabilité : [800504](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-0119](#)
- Packet affecté : -WINDOWS AND SERVICE PACK  
Résumé : Microsoft GDIPlus PNG Infinite Loop Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [800700](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:N/I:N/A:C/\)](#).  
Références : [CVE-2009-1511](#)
- Résumé : SMB Registry : Windows Service Pack version  
Script de test et informations relatives à cette vulnérabilité : [10401](#)  
Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : [\(AV:N/AC:L/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-1999-0662](#)
- Résumé : Microsoft Windows Address Book Insecure Library Loading Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [801457](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-3143](#) , [CVE-2010-3147](#)
- Packet affecté : -WINDOWS MEDIA PLAYER  
Résumé : Microsoft Windows Media Player MID File Integer Overflow Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [900336](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-1331](#)
- Packet affecté : -INTERNET EXPLORER  
Résumé : MS Internet Explorer Remote Code Execution Vulnerability (981374)  
Script de test et informations relatives à cette vulnérabilité : [800176](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0806](#)
- Correctif manquant : [MS09-028](#)  
Résumé : Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution  
Script de test et informations relatives à cette vulnérabilité : [900097](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-1537](#)
- Packet affecté : -INTERNET EXPLORER  
Résumé : Microsoft Internet Explorer Remote Code Execution Vulnerability (979352)  
Script de test et informations relatives à cette vulnérabilité : [800429](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2010-0249](#)
- Packet affecté : -INTERNET EXPLORER  
Résumé : Microsoft Internet Explorer Denial Of Service Vulnerability - July09  
Script de test et informations relatives à cette vulnérabilité : [800669](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:N/I:N/A:C/\)](#).  
Références : [CVE-2009-2536](#) , [CVE-2009-1692](#)
- Correctif manquant : [954157](#)  
Résumé : Microsoft Windows Indeo Codec Multiple Vulnerabilities  
Script de test et informations relatives à cette vulnérabilité : [801090](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2009-4313](#) , [CVE-2009-4309](#) , [CVE-2009-4310](#) , [CVE-2009-4210](#) , [CVE-2009-4312](#) , [CVE-2009-4311](#)
- Résumé : Microsoft Windows TrueType Font Parsing Privilege Elevation Vulnerability  
Script de test et informations relatives à cette vulnérabilité : [802500](#)  
Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : [\(AV:N/AC:M/AU:N/C:C/I:C/A:C/\)](#).  
Références : [CVE-2011-3402](#)
- Résumé : Adobe Flash Player 9.0.115.0 and earlier vulnerability (Win)



- Script de test et informations relatives à cette vulnérabilité : [90019](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2007-5275](#) , [CVE-2008-1655](#) , [CVE-2007-6637](#) , [CVE-2007-6243](#) , [CVE-2007-6019](#) , [CVE-2008-1654](#)
- Résumé : MS Internet Explorer 'Style' Object Remote Code Execution Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [800727](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2009-3674](#) , [CVE-2009-3671](#) , [CVE-2009-3673](#) , [CVE-2009-3672](#) , [CVE-2009-2493](#)
  - Correctif manquant : [MS09-019](#)  
 Résumé : Cumulative Security Update for Internet Explorer (969897)  
 Script de test et informations relatives à cette vulnérabilité : [900364](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2007-3091](#) , [CVE-2009-1528](#) , [CVE-2009-1529](#) , [CVE-2009-1531](#) , [CVE-2009-1140](#) , [CVE-2009-1532](#) , [CVE-2009-1530](#) , [CVE-2009-1141](#)
  - Résumé : Microsoft Windows Progman Group Converter Insecure Library Loading Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [801456](#)  
 Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-3139](#)
  - Correctif manquant : [MS08-062](#)  
 Résumé : Windows Internet Printing Service Allow Remote Code Execution Vulnerability (953155)  
 Script de test et informations relatives à cette vulnérabilité : [900052](#)  
 Risque : 9.0 (Impact : 10.0, Exploitabilité : 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).  
 Références : [CVE-2008-1446](#)
  - Résumé : Windows Messenger is installed  
 Script de test et informations relatives à cette vulnérabilité : [11429](#)  
 Risque : 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).  
 Références : [CVE-2002-0228](#) , [CVE-1999-1484](#) , [CVE-2002-0472](#)
  - Correctif manquant : [981169](#)  
 Résumé : MS Internet Explorer 'VBScript' Remote Code Execution Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [800482](#)  
 Risque : 7.6 (Impact : 10.0, Exploitabilité : 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0483](#)
  - Résumé : Windows XP 'SPI\_GETDESKWALLPAPER' DoS Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [900724](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:N/I:N/A:C/).  
 Références : [CVE-2009-1808](#)
  - Packet affecté : -MICROSOFT EXPLORER  
 Résumé : Microsoft Explorer HTTPS Sessions Multiple Vulnerabilities (Windows)  
 Script de test et informations relatives à cette vulnérabilité : [802140](#)  
 Risque : 7.1 (Impact : 6.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:P/).  
 Références : [CVE-2008-7295](#)
  - Résumé : Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [800442](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-0232](#)
  - Résumé : Microsoft Windows win32k.sys Driver 'CreateDIBPalette()' BOF Vulnerability  
 Script de test et informations relatives à cette vulnérabilité : [902256](#)  
 Risque : 7.1 (Impact : 10.0, Exploitabilité : 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).  
 Références : [CVE-2010-2739](#)

## Configuration / Logiciel désactivé

Majeur

**Description :** Le logiciel de sécurité est désactivé

**Résolution :** Activer le produit

**Priorité :** Majeur

**Méthodologie :** boîte blanche

**Risque :** 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

**Informations :** WindowsFirewall - Domain profile



<b>Configuration / Exigences de complexité des mots de passe désactivées</b>	<b>Majeur</b>
<p><b>Description :</b> Les exigences de complexité des mots de passe permettent d'éviter l'utilisation de mots de passe simples</p> <p><b>Résolution :</b> Activer les exigences de complexité des mots de passe</p> <p><b>Priorité :</b> Majeur</p> <p><b>Méthodologie :</b> boîte blanche</p> <p><b>Risque :</b> 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : <u>(AV:N/AC:L/AU:N/C:P/I:P/A:P/)</u>.</p>	
<b>Configuration / Longueur minimale des mots de passe trop courte</b>	<b>Majeur</b>
<p><b>Description :</b> Un mot de passe trop court permet d'augmenter les chances de réussite d'une attaque par brute force</p> <p><b>Résolution :</b> Augmenter la longueur minimale des mots de passe (au moins 6 caractères)</p> <p><b>Priorité :</b> Majeur</p> <p><b>Méthodologie :</b> boîte blanche</p> <p><b>Risque :</b> 8.8 (Impact : 8.3, Exploitabilité : 10.0) CVSS : <u>(AV:N/AC:L/AU:N/C:P/I:P/A:P/)</u>.</p> <p><b>Informations :</b> 3</p>	
<b>Configuration / Compte local activé</b>	<b>Majeur</b>
<p><b>Description :</b> Compte local activé sur une machine membre d'un domaine</p> <p><b>Résolution :</b> Désactiver les comptes locaux</p> <p><b>Priorité :</b> Majeur</p> <p><b>Méthodologie :</b> boîte blanche</p> <p><b>Risque :</b> 8.1 (Impact : 8.3, Exploitabilité : 8.6) CVSS : <u>(AV:N/AC:M/AU:N/C:P/I:P/A:P/)</u>.</p> <p><b>Informations :</b> Vulnit</p>	
<b>Configuration / Mot de passe n'expirant jamais</b>	<b>Majeur</b>
<p><b>Description :</b> Le mot de passe n'expire jamais, ce qui permet d'augmenter les chances de réussite d'une attaque par brute force</p> <p><b>Résolution :</b> Retirer l'option permettant la non-expiration du mot de passe</p> <p><b>Priorité :</b> Majeur</p> <p><b>Méthodologie :</b> boîte blanche</p> <p><b>Risque :</b> 8.1 (Impact : 8.3, Exploitabilité : 8.6) CVSS : <u>(AV:N/AC:M/AU:N/C:P/I:P/A:P/)</u>.</p>	



**Informations** : Administrateur, Vulnit



# Annexes

## Annexe A: Glossaire

- **Cible** - terme générique qui caractérise un serveur, poste de travail, imprimante, routeur ou n'importe quel élément accessible du réseau.
- **Correctif** - *patch* en anglais. C'est une mise à jour corrigeant une ou plusieurs vulnérabilités. Elle s'applique à un système d'exploitation, une base de données, un programme ou un paquet (sous Unix).
- **CVSS** - Common Vulnerability Scoring System. C'est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. La métrique de base (*Base metric*) est explicitée par le vecteur de 6 lettres indiqué pour expliciter chaque risque.
- **DBMS** - *DataBase Management System*. Système de gestion de base de données en français.
- **Exploitabilité** - facilité à exploiter une vulnérabilité. Plus l'exploitabilité est élevée, plus les compétences requises pour exploiter la faille sont faibles et donc plus une menace a de chance de survenir.
- **Fonction** - la fonction du contrôle détermine la cause d'une vulnérabilité. Par exemple, une injection SQL a pour cause une erreur de développement, un mot de passe trivial découle d'un contrôle d'accès mal paramétré. La configuration d'un service peut également entraîner des fuites d'informations.
- **Impact** - effet potentiel sur la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.
- **Nom DNS** - (*Domain Name Server*). Nom obtenu par résolution inverse auprès du ou des serveurs DNS.
- **Nom Netbios** - Nom d'une machine appartenant à un domaine ou un groupe de travail.
- **Objet** - ce sur quoi porte la vulnérabilité : systèmes d'exploitation (comprenant les applications installées sur ces systèmes), bases de données, sites/serveurs web ou réseau.
- **Priorité** - les 3 niveaux (Élevé, Majeur, Critique) suggérés dans le rapport permettent de traiter en priorité les vulnérabilités de risque maximal, dites critiques. *Note* : toutes les vulnérabilités remontées dans ce rapport sont de risque élevé (note CVSS supérieure à 7) et doivent donc toutes être considérées.
- **Risque** - risque potentiel d'une menace exploitant la vulnérabilité. Le risque final d'une vulnérabilité prend également en compte le risque intrinsèque de la machine ciblée (c'est-à-dire la valeur des informations qui y sont stockées ou l'importance opérationnelle des services qu'elle fournit) et les contrôles pouvant venir diminuer ce risque (traces d'audit, plan de secours, etc). Le calcul du risque est explicité dans ce document (partie Métrique de base).
- **Vulnérabilité** - faille de sécurité pouvant compromettre la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.



## Annexe B: Outils d'audit

- **Aircrack** est une suite d'outils d'audit wifi permettant d'analyser la sécurité de points d'accès wifi. Auteur et mainteneur : Thomas d'Otreppe.
- **CSRF Scanner** est un logiciel open-source permettant de détecter des failles CSRF (Cross-Site Request Forgery) dans les formulaires. Auteur et mainteneur : VulnIT.
- **db2getprofile** (de la suite db2utils) récupère le profil d'accès aux bases de données DB2 et fournit en particulier la liste des instances et bases de données. Auteur et mainteneur : Patrik Karlsson.
- **dhcping** est un scanner de serveurs DHCP et BOOTP. Auteur et mainteneur : Edwin Groothuis.
- **dig** - fourni avec le package dnsutils - permet entre autres d'interroger un serveur DNS pour obtenir la liste des machines d'un domaine par transfert de zone. Auteur et mainteneur : Internet Systems Consortium, Inc (ISC).
- **flasm** désassemble les menus SWF pour y relever les liens vers les autres pages du site. Auteur et mainteneur : Ben Schleimer.
- **Medusa** permet de tester des identifiants de connexion sur de nombreux services (FTP, SSH, SNMP, SMTP...). Auteur et mainteneur : JoMo-Kun.
- **mit-krb5** implémente sous unix le protocole kerberos utilisé pour l'authentification au domaine (dans le cas des domaines gérés par un active directory à partir de Windows 2003). Auteur et mainteneur : Massachusetts Institute of Technology.
- **MSSQLScan** permet d'obtenir quelques informations sur les bases de données Microsoft SQL Server. Auteur et mainteneur : Patrik Karlsson.
- **nbtscan** reprend les fonctionnalités de la commande 'nbtstat' de Windows en fournissant une liste de tous les services Netbios ouverts. Auteur et mainteneur : Stephen Friedl.
- **netcat** permet d'établir des connexions réseaux et ajoute à telnet de nombreuses fonctionnalités intéressantes. Auteur et mainteneur : Giovanni Giacobbi.
- **Nmap** est un célèbre scanner de ports utilisé pour détecter quels sont les services ouverts sur les machines. Auteur et mainteneur : Gordon Lyon.
- **OpenVAS** intègre plusieurs milliers de tests sur l'application des correctifs (*patch management*) OS, applicatifs, DBMS, etc. Auteur et mainteneur : OpenVAS team.
- **rpcclient** permet d'accéder aux "tubes nommés" et d'exécuter des commandes MS RPC. Il fait partie de la suite Samba. Auteur et mainteneur : Samba team.
- **opwg** (faisant partie de la suite Oracle Auditing Tools) réalise une attaque par dictionnaire sur les bases de données Oracle. Auteur et mainteneur : Patrik Karlsson.
- **SidGuesser** permet de découvrir les instances Oracle lorsqu'elles ne sont pas transmises par le listener (attaque par dictionnaire). Auteur et mainteneur : Patrik Karlsson.
- **snpwalk** fait partie du package net-snmp et permet de parcourir les informations fournies par le protocole SNMP. Auteur et mainteneur : Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) comprend l'outil smbdumpusers permettant de lister les utilisateurs de Windows NT/2000. Auteur et mainteneur : Patrik Karlsson.
- **smbclient** est un équivalent du 'net use' de Windows et permet d'obtenir des informations sur les partages Windows. Auteur et mainteneur : Samba team.
- **sqlmap** est un outil open source de tests de pénétration qui automatise le processus de détection de failles d'injection SQL. Auteur et mainteneur : Bernardo Damele.
- **sslscan** détermine quels algorithmes de chiffrement un serveur SSL propose (typiquement dans le cas d'un site https). Auteur et mainteneur : Ian Ventura-Whiting.
- **tnscmd10g** permet de recenser les instances des bases de données Oracle (versions 10g et 11g incluses). Auteur : James W. Abendschan, Mainteneur : Saez Scheihing.
- **WhatWeb** identifie les systèmes de gestion de contenu (CMS), plateformes de blogs, stats / packages d'analyse, et les bibliothèques javascript. Auteur et mainteneur : Brendan Coles.
- **wdiff** est une interface de comparaison de fichiers sur une base de mot par mot. Auteur et mainteneur : Denver Gingerich.
- **XSS Scanner** est un logiciel open-source dédié à la détection d'injections XSS (Cross-Site Scripting). Auteur et mainteneur : VulnIT.

## Annexe C : Génération du rapport



- **La librairie eZ Components** a permis de générer en PHP l'ensemble des graphiques contenus dans ce rapport. Auteur et mainteneur : eZ Systems.
- **PostgreSQL** est une base de données relationnelle. Auteur et mainteneur : PostgreSQL Global Development Group.
- **wKHTMLtopdf** (lire : WebKit HTML to PDF) combine la force du moteur de rendu XHTML/CSS WebKit (utilisé par Chrome et Safari par exemple) et sa librairie de rendu PDF. Auteur et mainteneur : Jakob Truelsen.



---

## Légal

En respect de la LCEN (Loi pour la Confiance dans l'Economie Numérique, article 323-3-1 du 21 juin 2004), la solution VulnIT est exclusivement mise à disposition d'entreprises légitimes et d'utilisateurs dont la fonction justifie la réalisation d'audits de sécurité.

En acceptant la licence d'utilisation de VulnIT, l'utilisateur s'engage à respecter la loi Godfrain du 6 janvier 1988 punissant l'intrusion non autorisée dans un système informatique.

---

## Copyright

Le nom VulnIT, le logo et autres éléments graphiques relatifs à VulnIT sont déposés.

---