

[VULNIT]

Vulnerability
Identification Tool

Audit report

1 March 2012, 16:27:07 - UTC

Tool version	4.5
Number of scanned machines	5
Number of identified vulnerabilities	38

Table of contents

Table of contents	2
Introduction	3
Methodology	3
Risk assessment	3
Priorization of vulnerabilities	3
Management Report	4
Vulnerabilities ordered by priority	4
Vulnerabilities ordered by function and object	5
Critical priority vulnerabilities, by function and object	6
Number of missing patches, ordered by IP and objet	7
Technical report	8
Inventory	8
Summary	10
WORKGROUP\OWASPBWA (192.168.1.21)	12
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	49
Annex A: Glossary	49
Annex B: Auditing tools	50
Annex C: Report generation	50
Legal notice	52
Copyright statement	52



Introduction

The audit tool VulnIT enhances the identification of potential IT security vulnerabilities and the risk they could generate if they were exploited by an evil attacker.

The first part of this report brings a brief and executive summary of the security vulnerabilities identified. The second part lists all these vulnerabilities coupled with an assessment of their potential risks and a disclosure to help you understand and remediate them. Finally, the first appendix lists all the servers and services discovered during the scan.

Methodology

This report is not meant to be exhaustive and thus, does not replace the analysis an expert in pentesting could make. Moreover, all the information contained in this report should be validated by the administrator of the system targeted by the audit, in order to avoid any vulnerability mistakenly identified by the tool ("false positive").

Risk assessment

The risk assessment used in this report for rating each vulnerability relies on the Common Vulnerability Scoring System (CVSS) which considers two factors:

- the potential impact of an attack exploiting this vulnerability, in terms of availability of the application, confidentiality and integrity of the information,
- the exploitability of the vulnerability, as an easy-to-exploit vulnerability increases the number of potential attackers and thus, the likelihood of an attack.

The CVSS ratings (base rating, impact and exploitability) spread between 0 and 10.

Only the high risk vulnerabilities (CVSS base score greater than 7) are raised in this report and thus should all be tackled carefully.

Priorization of vulnerabilities

The priority suggested for each vulnerability falls into three levels: critical priority (CVSS base score equals 10), major (base score between 8 and 10) or high (base score between 7 and 8).

In order to determine the real risk induced by each vulnerability, the potential impact must be weighted by the asset value (for instance, the operational criticality of an application or the value of the information that could be compromised), and the exploitability, by the company exposure (for instance, financial activities motivate more attacks than others).

Finally, these risks may be mitigated by specific controls, either preventive, dissuasive or palliative.



Management Report

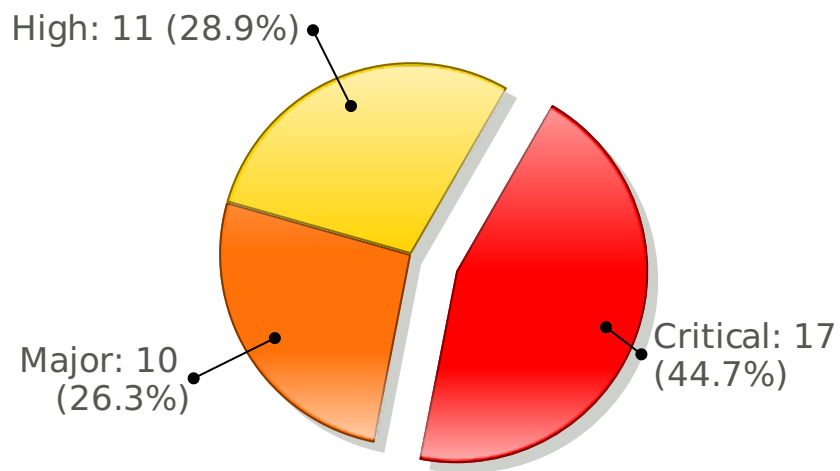
Summary:

Among the 5 tested servers, 5 have at least one vulnerability. **5** of them require all your attention because **critical priority vulnerabilities have been detected on them.**

These vulnerabilities are graphically presented below and detailed in the technical report.

Vulnerabilities ordered by priority

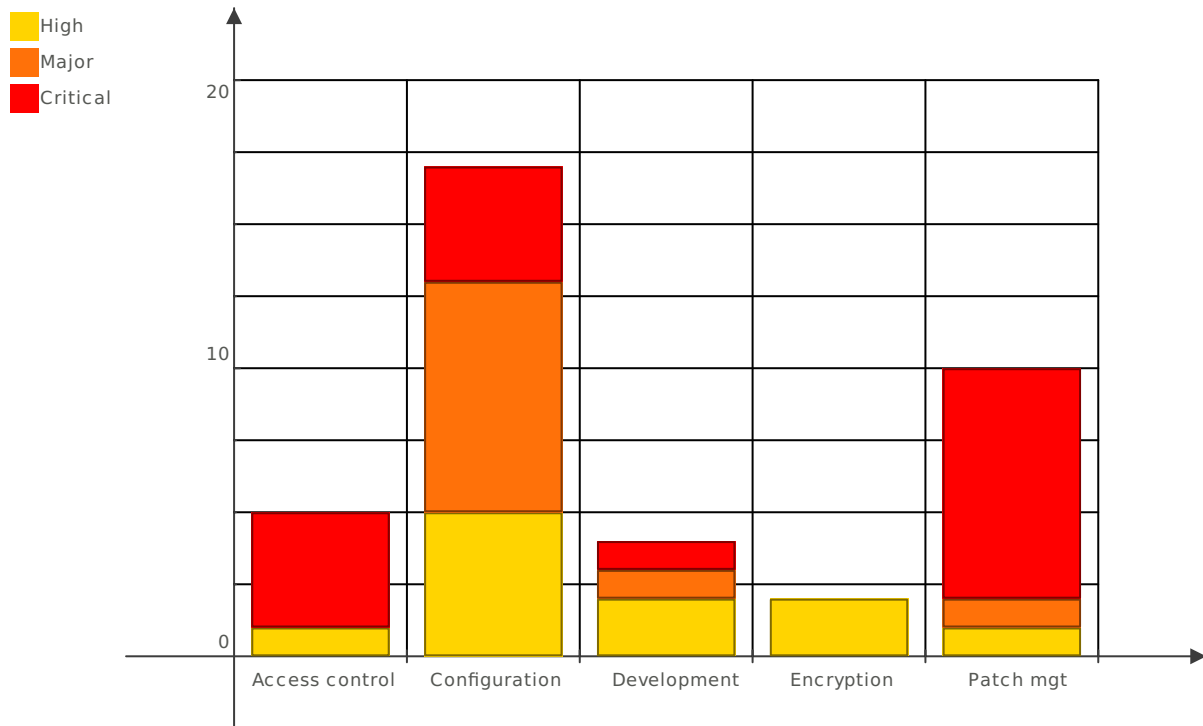
This chart shows the number of identified vulnerabilities ordered by priority.



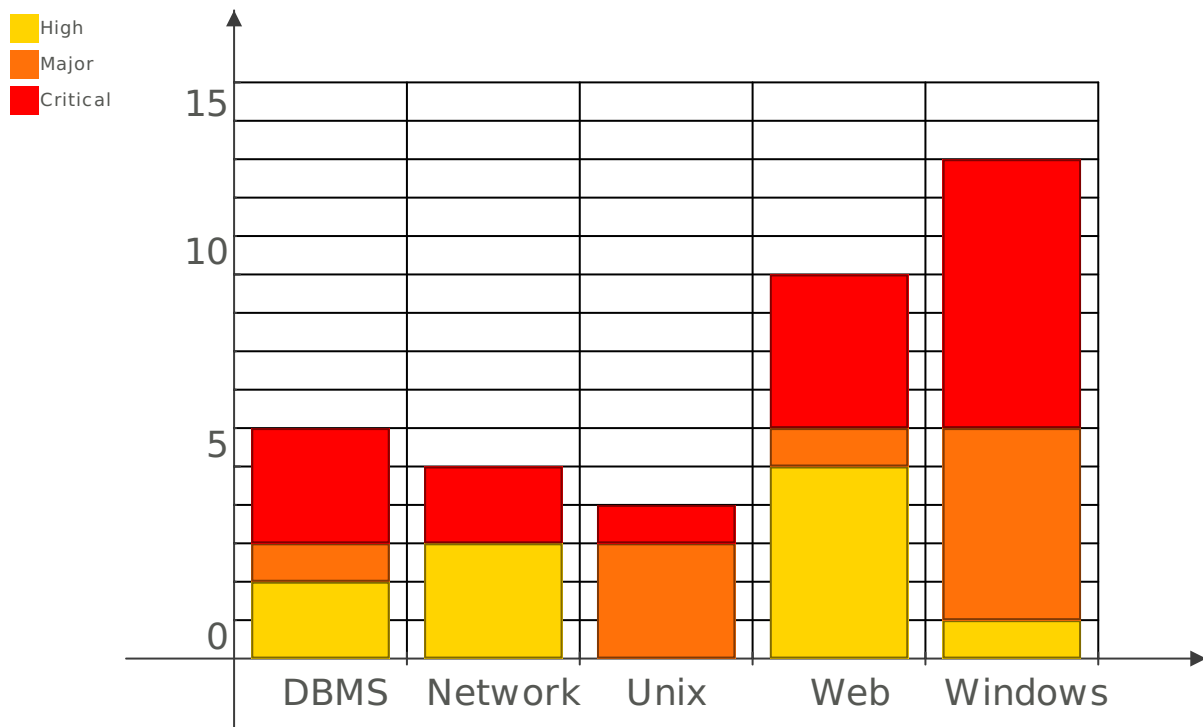


Vulnerabilities ordered by function and object

This chart shows the number of vulnerabilities ordered by control function.

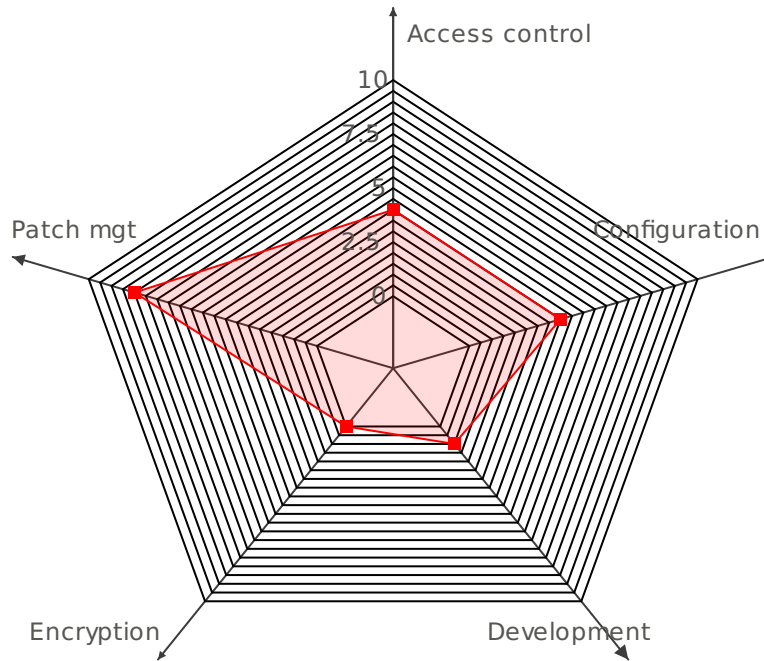


This chart shows the number of vulnerabilities ordered by control object.

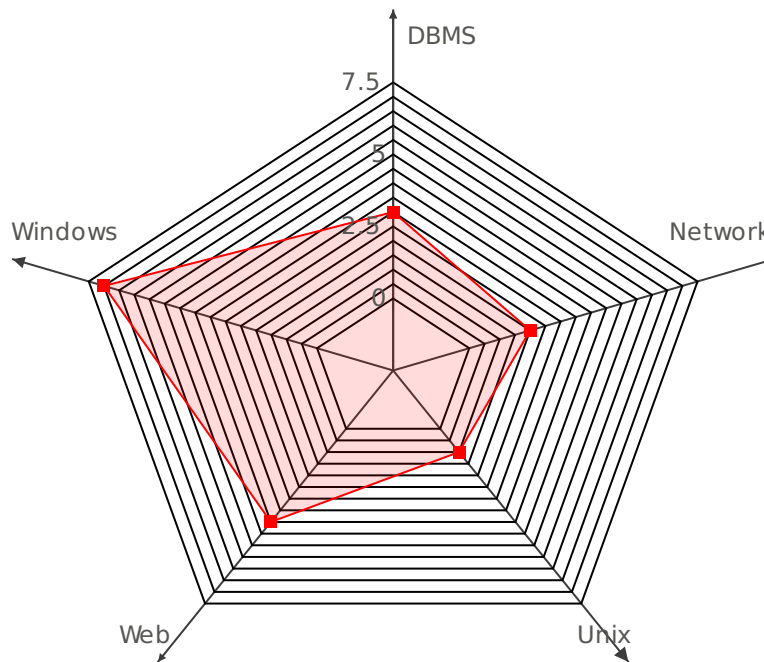


Critical priority vulnerabilities, by function and object

This chart shows the number of critical priority vulnerabilities ordered by control function.



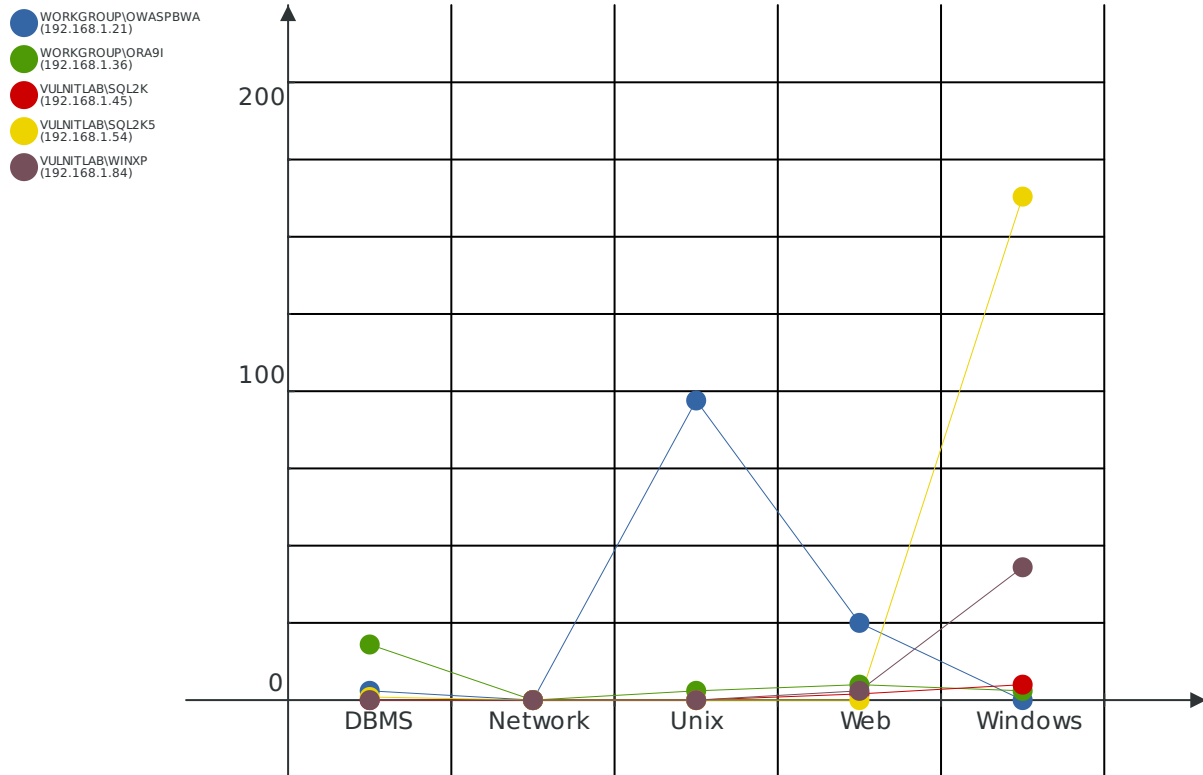
This chart shows the number of critical priority vulnerabilities classified by control object.





Number of missing patches, ordered by IP and objet

This chart presents the number of missing patches for each target ordered by control object.





Technical report

Inventory

VULNITLAB\SQL2K (192.168.1.45)

Last scanned: 2012-02-22 17:49:02

Validated administrator account: no

Target tested: yes

Number of vulnerabilities:

- Critical : 7
- Major : 0
- High : 2
- Open ports : 27

Information on remote machine:

- DNS : sql2k
- NetBios : VULNITLAB\SQL2K

Services :

- 7/tcp : echo - not tested
- 7/udp : echo - not tested
- 9/tcp : discard server
- 13/udp : daytime - not tested
- 13/tcp : daytime - not tested
- 17/tcp : Quote of the Day - not tested
- 19/tcp : ttytst source Character Generator - not tested
- 25/tcp : SMTP - Simple Mail Transfer Protocol
- 42/tcp : WINS - Windows Internet Naming Service - not tested
- 53/tcp : DNS - Domain Name Server
- 80/tcp : HTTP - World Wide Web - not tested
- 135/udp : RPC - Microsoft EPMAP - not tested
- 135/tcp : RPC - Microsoft EPMAP - not tested
- 137/udp : Netbios name service - not tested
- 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 - not tested
- 1029/tcp : ms-lsa - not tested
- 1033/tcp : netinfo-local - not tested
- 1036/tcp : pcg-radar - not tested
- 1042/tcp : blah11 - not tested
- 1433/tcp : MSSQL - Microsoft SQL Server
- 1434/udp : MSSQL - Microsoft SQL Monitor - not tested
- 3372/tcp : MDTC - Microsoft Distributed Transaction Coordinator - not tested

WORKGROUP\OWASPBWA (192.168.1.21)

Last scanned: 2012-03-01 15:50:03

Validated administrator account: yes

Target tested: yes

**Number of vulnerabilities:**

- Critical : 4
- Major : 4
- High : 5
- Open ports : 6

Information on remote machine:

- 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 : Unknown
- NetBios : WORKGROUP\OWASPBWA

Services :

- 22/tcp : SSH - Secure Shell Login
- 80/tcp : HTTP - World Wide Web - not tested
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing
- 5001/tcp : complex-link - not tested
- 8080/tcp : HTTP Alternate - not tested

WORKGROUP\ORA9I (192.168.1.36)

Last scanned: 2012-02-29 16:57:02

Validated administrator account: no

Target tested: yes

Number of vulnerabilities:

- Critical : 4
- Major : 0
- High : 3
- Open ports : 13

Information on remote machine:

- DNS : ora9i
- NetBios : WORKGROUP\ORA9I

Services :

- 80/tcp : HTTP - World Wide Web - not tested
- 135/tcp : RPC - Microsoft EPMAP - not tested
- 137/udp : Netbios name service - not tested
- 139/tcp : NETBIOS Services
- 443/tcp : HTTPS - Secure HTTP
- 445/tcp : SMB - Microsoft File Sharing
- 1029/tcp : ms-lsa - not tested
- 1034/tcp : ActiveSync Notifications - not tested
- 1521/tcp : Oracle
- 1808/tcp : oracle-vp2 - not tested
- 2030/tcp : device2 - not tested
- 2100/tcp : FTP - File Transfer Protocol



- 8080/tcp : HTTP - World Wide Web - not tested

VULNITLAB\WINXP (192.168.1.84)

Last scanned: 2012-03-01 15:37:02

Validated administrator account: yes

Target tested: yes

Number of vulnerabilities:

- Critical : 1
- Major : 5
- High : 0
- Open ports : 3

Information on remote machine:

- DNS : WINXP
- NetBios : VULNITLAB\WINXP

Services :

- 137/udp : Netbios name service - not tested
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing

VULNITLAB\SQL2K5 (192.168.1.54)

Last scanned: 2011-12-07 15:30:03

Validated administrator account: no

Target tested: yes

Number of vulnerabilities:

- Critical : 1
- Major : 1
- High : 1
- Open ports : 5

Information on remote machine:

- DNS : sql2k5
- NetBios : VULNITLAB\SQL2K5

Services :

- 135/tcp : RPC - Microsoft EPMAP - not tested
- 139/tcp : NETBIOS Services
- 445/tcp : SMB - Microsoft File Sharing
- 1027/tcp : exosee - not tested
- 1433/tcp : MSSQL - Microsoft SQL Server

Summary

- WORKGROUP\OWASPBWA (192.168.1.21) - Access control / Trivial Auth. Account -



- **Critical**
- WORKGROUP\OWASPBWA (192.168.1.21) - Patch mgt / Unix patch management - **Critical**
- WORKGROUP\OWASPBWA (192.168.1.21) - Development / SQLi - **Critical**
- WORKGROUP\OWASPBWA (192.168.1.21) - Patch mgt / Web patch management - **Critical**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [device] Device has world permissions - **Major**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [account] Bad permissions on the parent home directory. - **Major**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / [permissions] File is setgid. - **Major**
- WORKGROUP\OWASPBWA (192.168.1.21) - Development / XSS - **Major**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / Users list available - **High**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / Fingerprint DB - **High**
- WORKGROUP\OWASPBWA (192.168.1.21) - Development / FI - **High**
- WORKGROUP\OWASPBWA (192.168.1.21) - Configuration / PWD Capture - **High**
- WORKGROUP\OWASPBWA (192.168.1.21) - Development / CSRF - **High**
- WORKGROUP\ORA9I (192.168.1.36) - Access control / Trivial account - **Critical**
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Database patch management - **Critical**
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Windows patch management - **Critical**
- WORKGROUP\ORA9I (192.168.1.36) - Patch mgt / Web patch management - **Critical**
- WORKGROUP\ORA9I (192.168.1.36) - Encryption / FTP service - **High**
- WORKGROUP\ORA9I (192.168.1.36) - Configuration / Instance list available - **High**
- WORKGROUP\ORA9I (192.168.1.36) - Encryption / Weak SSL encryption - **High**
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Trivial account - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Users list available - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Open share folder - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / SNMP community (write) - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Windows patch management - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / RPC information leakage - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / Discard service - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Configuration / SNMP community (read) - **Critical**
- VULNITLAB\SQL2K (192.168.1.45) - Access control / Open mail relay - **High**
- VULNITLAB\SQL2K (192.168.1.45) - Patch mgt / Web patch management - **High**
- VULNITLAB\SQL2K5 (192.168.1.54) - Patch mgt / Windows patch management - **Critical**
- VULNITLAB\SQL2K5 (192.168.1.54) - Patch mgt / Database patch management - **Major**
- VULNITLAB\SQL2K5 (192.168.1.54) - Configuration / Instance list available - **High**
- VULNITLAB\WINXP (192.168.1.84) - Patch mgt / Windows patch management - **Critical**
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Software disabled - **Major**
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Passwords complexity requirements disable - **Major**
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Minimum password length too low - **Major**
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Local user account enabled - **Major**
- VULNITLAB\WINXP (192.168.1.84) - Configuration / Password never expires - **Major**



WORKGROUP\OWASPBWA (192.168.1.21)

Access control / Trivial Auth. Account

Critical

Description: A trivial authentication account was found on this page of the website

Remediation: Change the password of the account to a more complicated one

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

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

- Page: <http://192.168.1.21/mutillidae/index.php?page=login.php>
Method: POST
Information : [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>
Method: POST
Information : [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>
Method: POST
Information : [POST(Fuzz) - <http://192.168.1.21/WackoPicko/admin/index.php?page=login>
Params: {#adminname:admin#password:admin}
Cookies: {%PHPSESSID:k56vbc1uf3dnabf5kcdbcecoc5}]

Patch mgt / Unix patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: white box

- Missing patch: [USN-1210-1](#)
Summary: Ubuntu Update for firefox USN-1210-1
Test script and information relative to this vulnerability: [840756](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2011-2999](#), [CVE-2011-3000](#), [CVE-2011-2996](#), [CVE-2011-2372](#), [CVE-2011-3001](#), [CVE-2011-2995](#)
- Missing patch: [USN-1184-1](#)
Summary: Ubuntu Update for firefox USN-1184-1
Test script and information relative to this vulnerability: [840727](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2011-2984](#), [CVE-2011-2982](#), [CVE-2011-2378](#), [CVE-2011-2981](#), [CVE-2011-0084](#), [CVE-2011-2983](#)
- Missing patch: [USN-1263-2](#)
Summary: Ubuntu Update for openjdk-6 USN-1263-2
Test script and information relative to this vulnerability: [840872](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Affected package: -SUN JAVA JRE/JDK
Summary: Sun Java JRE Multiple Vulnerabilities (Linux)
Test script and information relative to this vulnerability: [902168](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-1423](#), [CVE-2010-0886](#), [CVE-2010-0887](#)



- Missing patch: [USN-1010-1](#)
Summary: Ubuntu Update for openjdk-6, openjdk-6b18 vulnerabilities USN-1010-1
Test script and information relative to this vulnerability: [840527](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1049-2](#)
Summary: Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1049-2
Test script and information relative to this vulnerability: [840609](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1154-1](#)
Summary: Ubuntu Update for openjdk-6 USN-1154-1
Test script and information relative to this vulnerability: [840683](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1112-1](#)
Summary: Ubuntu Update for firefox USN-1112-1
Test script and information relative to this vulnerability: [840640](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1149-1](#)
Summary: Ubuntu Update for firefox USN-1149-1
Test script and information relative to this vulnerability: [840684](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1000-1](#)
Summary: Ubuntu Update for Linux kernel vulnerabilities USN-1000-1
Test script and information relative to this vulnerability: [840523](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1079-1](#)
Summary: Ubuntu Update for openjdk-6 vulnerabilities USN-1079-1
Test script and information relative to this vulnerability: [840607](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1049-1](#)
Summary: Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1049-1
Test script and information relative to this vulnerability: [840604](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1263-1](#)
Summary: Ubuntu Update for icedtea-web USN-1263-1
Test script and information relative to this vulnerability: [840805](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [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](#)
- Missing patch: [USN-1267-1](#)
Summary: Ubuntu Update for freetype USN-1267-1



- Test script and information relative to this vulnerability: [840810](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-3439](#) , [CVE-2011-3256](#)
- Missing patch: [USN-1019-1](#)
 Summary: Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-1019-1
 Test script and information relative to this vulnerability: [840553](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [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](#)
 - Missing patch: [USN-1085-1](#)
 Summary: Ubuntu Update for tiff vulnerabilities USN-1085-1
 Test script and information relative to this vulnerability: [840610](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [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](#)
 - Missing patch: [USN-1251-1](#)
 Summary: Ubuntu Update for firefox USN-1251-1
 Test script and information relative to this vulnerability: [840801](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-3004](#) , [CVE-2011-3650](#) , [CVE-2011-3647](#) , [CVE-2011-3648](#)
 - Missing patch: [USN-1334-1](#)
 Summary: Ubuntu Update for libxml2 USN-1334-1
 Test script and information relative to this vulnerability: [840868](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-3905](#) , [CVE-2011-3919](#) , [CVE-2011-2821](#) , [CVE-2011-0216](#) , [CVE-2011-2834](#)
 - Missing patch: [USN-1011-3](#)
 Summary: Ubuntu Update for Xulrunner vulnerability USN-1011-3
 Test script and information relative to this vulnerability: [840528](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-3765](#)
 - Missing patch: [USN-1013-1](#)
 Summary: Ubuntu Update for freetype vulnerabilities USN-1013-1
 Test script and information relative to this vulnerability: [840532](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-3311](#) , [CVE-2010-3814](#) , [CVE-2010-3855](#)
 - Missing patch: [USN-997-1](#)
 Summary: Ubuntu Update for Firefox and Xulrunner vulnerabilities USN-997-1
 Test script and information relative to this vulnerability: [840518](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-3177](#) , [CVE-2010-3182](#) , [CVE-2010-3178](#) , [CVE-2010-3176](#) , [CVE-2010-3175](#) , [CVE-2010-3179](#) , [CVE-2010-3180](#) , [CVE-2010-3183](#)
 - Missing patch: [USN-1085-2](#)
 Summary: Ubuntu Update for tiff regression USN-1085-2
 Test script and information relative to this vulnerability: [840613](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-2630](#) , [CVE-2010-2595](#) , [CVE-2010-2597](#) , [CVE-2010-2598](#) , [CVE-2011-0191](#) , [CVE-2010-2482](#) , [CVE-2010-3087](#)
 - Missing patch: [USN-1153-1](#)
 Summary: Ubuntu Update for libxml2 USN-1153-1
 Test script and information relative to this vulnerability: [840679](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-1944](#)
 - Summary: Perl Safe Module 'reval()' and 'rdo()' CVE-2010-1447 Restriction-Bypass Vulnerabilities
 Test script and information relative to this vulnerability: [100673](#)
 Risk: 8.5 (Impact: 10.0, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).
 References: [CVE-2010-1447](#)
 - Missing patch: [USN-1129-1](#)
 Summary: Ubuntu Update for perl USN-1129-1
 Test script and information relative to this vulnerability: [840647](#)
 Risk: 8.5 (Impact: 10.0, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).
 References: [CVE-2011-1487](#) , [CVE-2010-4411](#) , [CVE-2010-1168](#) , [CVE-2010-2761](#) , [CVE-2010-4410](#) , [CVE-2010-1447](#)
 - Missing patch: [USN-1012-1](#)
 Summary: Ubuntu Update for cups, cupsys vulnerability USN-1012-1
 Test script and information relative to this vulnerability: [840531](#)
 Risk: 7.9 (Impact: 10.0, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:C/A:C/).



- References: [CVE-2010-2941](#)
- Missing patch: [USN-1041-1](#)
 Summary: Ubuntu Update for linux, linux-ec2 vulnerabilities USN-1041-1
 Test script and information relative to this vulnerability: [840565](#)
 Risk: 7.9 (Impact: 9.2, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:N/).
 References: [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](#)
 - Missing patch: [USN-1199-1](#)
 Summary: Ubuntu Update for apache2 USN-1199-1
 Test script and information relative to this vulnerability: [840734](#)
 Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
 References: [CVE-2011-3192](#)
 - Summary: Apache httpd Web Server Range Header Denial of Service Vulnerability
 Test script and information relative to this vulnerability: [901203](#)
 Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
 References: [CVE-2011-3192](#)
 - Missing patch: [USN-1088-1](#)
 Summary: Ubuntu Update for krb5 vulnerability USN-1088-1
 Test script and information relative to this vulnerability: [840616](#)
 Risk: 7.6 (Impact: 10.0, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-0284](#)
 - Missing patch: [USN-1335-1](#)
 Summary: Ubuntu Update for t1lib USN-1335-1
 Test script and information relative to this vulnerability: [840866](#)
 Risk: 7.6 (Impact: 10.0, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-2642](#), [CVE-2011-1554](#), [CVE-2011-1553](#), [CVE-2011-1552](#)
 - Missing patch: [USN-1082-1](#)
 Summary: Ubuntu Update for pango1.0 vulnerabilities USN-1082-1
 Test script and information relative to this vulnerability: [840602](#)
 Risk: 7.6 (Impact: 10.0, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-0421](#), [CVE-2011-0064](#), [CVE-2011-0020](#)
 - Missing patch: [USN-1126-2](#)
 Summary: Ubuntu Update for php5 USN-1126-2
 Test script and information relative to this vulnerability: [840636](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [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](#)
 - Affected package: -SUN JAVA SE JRE
 Summary: Oracle Java SE Multiple Vulnerabilities (Linux)
 Test script and information relative to this vulnerability: [800500](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [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](#)
 - Affected package: -SAFE
 Summary: Perl Safe Module 'reval()' and 'rdo()' Restriction-Bypass Vulnerabilities
 Test script and information relative to this vulnerability: [100672](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2010-1168](#)
 - Missing patch: [USN-1231-1](#)
 Summary: Ubuntu Update for php5 USN-1231-1
 Test script and information relative to this vulnerability: [840782](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2010-1914](#), [CVE-2011-2202](#), [CVE-2011-2483](#), [CVE-2011-1938](#), [CVE-2011-3267](#), [CVE-2010-2484](#), [CVE-2011-1657](#), [CVE-2011-3182](#)
 - Affected package: -SAMBA
 Summary: Samba SID Parsing Remote Buffer Overflow Vulnerability
 Test script and information relative to this vulnerability: [100803](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2010-3069](#)
 - Missing patch: [USN-1108-2](#)
 Summary: Ubuntu Update for dhcp3 USN-1108-2
 Test script and information relative to this vulnerability: [840645](#)



- Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
- References: [CVE-2011-0997](#)
- Missing patch: [USN-1007-1](#)
Summary: Ubuntu Update for nss vulnerabilities USN-1007-1
Test script and information relative to this vulnerability: [840520](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 - Missing patch: [USN-1126-1](#)
Summary: Ubuntu Update for php5 USN-1126-1
Test script and information relative to this vulnerability: [840646](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 - Missing patch: [USN-1158-1](#)
Summary: Ubuntu Update for curl USN-1158-1
Test script and information relative to this vulnerability: [840685](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 - Missing patch: [USN-1252-1](#)
Summary: Ubuntu Update for tomcat6 USN-1252-1
Test script and information relative to this vulnerability: [840803](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 - Missing patch: [USN-1108-1](#)
Summary: Ubuntu Update for dhcp3 vulnerability USN-1108-1
Test script and information relative to this vulnerability: [840633](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 - Missing patch: [USN-1009-1](#)
Summary: Ubuntu Update for glibc, eglibc vulnerabilities USN-1009-1
Test script and information relative to this vulnerability: [840525](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:I/C/A/C/).
 - Missing patch: [USN-1080-1](#)
Summary: Ubuntu Update for linux vulnerabilities USN-1080-1
Test script and information relative to this vulnerability: [840600](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:I/C/A/C/).
 - Missing patch: [USN-1009-2](#)
Summary: Ubuntu Update for eglibc, glibc vulnerability USN-1009-2
Test script and information relative to this vulnerability: [840567](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:I/C/A/C/).

Development / SQLi

Critical

Description: A SQL injection attack consists of insertion or injection of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Remediation: Primary Defenses: use of Prepared Statements (Parameterized Queries), use of Stored Procedures, escaping all user-supplied input. Additional Defenses: enforce least privilege and perform white list input validation.

Priority: Critical



Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2010 A1, OWASP prevention sheet, CWE-89

- Page: <http://192.168.1.21/mutillidae/index.php?page=register.php>
Method: POST
Attacked parameter: user_name
Information : 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>
Method: POST
Attacked parameter: user_name
Information : 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>
Method: POST
Attacked parameter: view_user_name
Information : 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>
Method: POST
Attacked parameter: show_only_user
Information : 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>
Method: GET
Attacked parameter: forwardurl
Information : forwardurl=-6036' OR 7735=SLEEP(6) AND 'VULNITsatyf'='VULNITsatyf
- Page: <http://192.168.1.21/mutillidae/index.php>
Method: GET
Attacked parameter: uid
Cookie: uid=1
Information : [Cookie -> -4093' OR 6668=SLEEP(6) AND 'VULNITsIKow'='VULNITsIKow]
- Page: <http://192.168.1.21/mutillidae/index.php?page=dns-lookup.php>
Method: POST
Attacked parameter: uid
Cookie: uid=1
Information : [Cookie -> -8329' OR 721=SLEEP(6) AND 'VULNITsTnUG'='VULNITsTnUG]
- Page: <http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php>
Method: POST
Attacked parameter: uid
Cookie: uid=1
Information : [Cookie -> -184' OR 1192=SLEEP(6) AND 'VULNITsPenH'='VULNITsPenH]
- Page: <http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php>
Method: POST
Attacked parameter: uid
Cookie: uid=1
Information : [Cookie -> -9448' OR 9272=SLEEP(6) AND 'VULNITsVtDw'='VULNITsVtDw]
- Page: <http://192.168.1.21/WackoPicko/users/login.php>
Method: POST
Attacked parameter: username
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
Information : username=-8709' OR 7409=SLEEP(6) AND 'VULNITsUMIJ'='VULNITsUMIJ
- Page: <http://192.168.1.21/vicnum/vicnum5.php>
Method: POST
Attacked parameter: player
Information : player=-7453' OR 6591=SLEEP(6) AND 'VULNITsQEzb'='VULNITsQEzb

Patch mgt / Web patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative



security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: white box

- Affected package: -WORDPRESS
Summary: WordPress 'wp-admin' Multiple Vulnerabilities - Aug09
Test script and information relative to this vulnerability: [900915](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-2853](#) , [CVE-2009-2854](#)
- Affected package: -WORDPRESS
Summary: WordPress cat Parameter Directory Traversal Vulnerability
Test script and information relative to this vulnerability: [800124](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2008-4769](#)
- Affected package: -WORDPRESS
Summary: WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability
Test script and information relative to this vulnerability: [900183](#)
Risk: 8.5 (Impact: 10.0, Exploitability: 6.8) CVSS : (AV:N/AC:M/AU:S/C:C/I:C/A:C/).
References: [CVE-2008-5695](#)
- Affected package: - OF WORDPRESS
Summary: WordPress Multiple Vulnerabilities
Test script and information relative to this vulnerability: [900219](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: [CVE-2008-3747](#)
- Affected package: -PHP
Summary: PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability
Test script and information relative to this vulnerability: [100684](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: [CVE-2010-2225](#)

Configuration / [device] Device has world permissions

Major

Description: Devices that have improper (world) permissions might be accessed by any system user. This might open security holes if these are shared devices or hold binaries (disks for example).

Remediation: The administrator should properly set device access (using group configuration to provide access to a device to multiple users, for example).

Priority: Major

Methodology: white box

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

Information : [/dev/fuse, /dev/log, /dev/ptmx, /dev/rfkill]

Configuration / [account] Bad permissions on the parent home directory.

Major

Description: The home directory of the listed login ID has group write permission, world write permission or both enabled. This allows new files to be added (and existing files potentially removed) by others.

Remediation: The write permissions should be removed.

Priority: Major



Methodology: white box

Risk: 8.5 (Impact: 9.2, Exploitability: 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:C/A:N/).

Information : [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] File is setgid.

Major

Description: The indicated file has the setgid (group) bit set, but it should not have it.

Remediation: .This should be changed by using 'chmod g-s file' where 'file' is the indicated file. The system should be checked for signs of intrusion.

Priority: Major

Methodology: white box

Risk: 8.5 (Impact: 9.2, Exploitability: 8.0) CVSS : (AV:N/AC:S/AU:S/C:C/I:C/A:N/).

Information :

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

Development / XSS

Major

Description: Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Remediation: Output Encoding: a technique used to ensure that characters are treated as data, not as characters that are relevant to the interpreter's parser. There are lots of different types of escaping, sometimes confusingly called output encoding. Some of these techniques define a special escape character, and other techniques have a more sophisticated syntax that involves several characters.

Priority: Major

Methodology: black box

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

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

- Page: <http://192.168.1.21/vicnum/vicnum5.php>
Method: POST
Attacked parameter: player
Information : player=<script>alert(331559492711322129638300)</script>
- Page: <http://192.168.1.21/WackoPicko/piccheck.php>
Method: POST
Attacked parameter: name
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
Information : name=<script>alert(331559492711322129319722)</script>
- Page: <http://192.168.1.21/WackoPicko/pictures/search.php>
Method: GET
Attacked parameter: query
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
Information : query=<script>alert(331559492711322129318918)</script>
- Page: <http://192.168.1.21/mutillidae/index.php?page=login.php>



- Method: POST
 Attacked parameter: user_name
 Information : user_name=<script>alert(331559492711322127789288)</script>
- Page: <http://192.168.1.21/mutillidae/index.php?page=user-info.php>
 Method: POST
 Attacked parameter: password
 Information : password=<script>alert(331559492711322127790579)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php>
 Method: POST
 Attacked parameter: input_from_form
 Information : input_from_form=<script>alert(331559492711322127791956)</script>
 - Page: <http://192.168.1.21/WackoPicko/guestbook.php>
 Method: POST
 Attacked parameter: comment
 Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
 Information : comment=<script>alert(331559492711322129321736)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=register.php>
 Method: POST
 Attacked parameter: password
 Information : password=<script>alert(331559492711322127788820)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=register.php>
 Method: POST
 Attacked parameter: user_name
 Information : user_name=<script>alert(331559492711322127788705)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=user-info.php>
 Method: POST
 Attacked parameter: view_user_name
 Information : view_user_name=<script>alert(331559492711322127790383)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php>
 Method: POST
 Attacked parameter: show_only_user
 Information : show_only_user=<script>alert(331559492711322127792521)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php>
 Method: GET
 Attacked parameter: php_file_name
 Information : php_file_name=<script>alert(331559492711322127793620)</script>
 - Page: <http://192.168.1.21/vicnum/cgi-bin/vicnum1.pl>
 Method: POST
 Attacked parameter: player
 Information : player=<script>alert(331559492711322129637331)</script>
 - Page: <http://192.168.1.21/mutillidae/index.php?page=login.php>
 Method: POST
 Attacked parameter: password
 Information : password=<script>alert(331559492711322127789345)</script>

Configuration / Users list available

High

Description: The server version and configuration enables to obtain the list of its users.

Remediation: Migrate to a more recent operating system.

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N).

Information : [nobody, None, user, root]

Configuration / Fingerprint DB

High

Description: Giving information on the database system used may help an attacker (error messages...)



Remediation: Do not display error messages giving information on the database used

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

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

Development / FI

High

Description: File inclusion allows an attacker to send a malicious program on the application server or disclose information from the application server.

Remediation: File inclusion can be avoided by protecting the objects parameters references (internal or external). It may also be restricted by appropriate server configurations.

Priority: High

Methodology: black box

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

References: [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
Attacked parameter: page
Cookie: showhints=1
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=footer.php
Attacked parameter: page
- Page: <http://192.168.1.21/mutillidae/?page=/etc/passwd>
Attacked parameter: page
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.2590453632606361
Attacked parameter: page
Cookie: uid=1
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.9298311197090497
Attacked parameter: page
Cookie: uid=1;showhints=1
- Page: <http://192.168.1.21/mutillidae/index.php?page=/etc/passwd>
Attacked parameter: page
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.01902171156707999
Attacked parameter: page
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=/etc/passwd



- Attacked parameter: php_file_name
 • Page: <http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php>
 Attacked parameter: text_file_name

Configuration / PWD Capture

High

Description: An form authentication password is sent over HTTP, which enables interception or spoofing.

Remediation: Encrypt the communication (using HTTPS).

Priority: High

Methodology: black box

Risk: 7.3 (Impact: 9.2, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:C/).

References: [OWASP 2010 A9OWAP Prevention sheet, CWE-319](#)

- Page: <http://192.168.1.21/mutillidae/index.php?page=user-info.php>
Attacked parameter: password
- Page: <http://192.168.1.21/bodgeit/register.jsp>
Attacked parameter: password1
Cookie: JSESSIONID=9AAC0580FF9958EE4B5AF33FAAD75974
- Page: <http://192.168.1.21/WackoPicko/users/register.php>
Attacked parameter: password
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: <http://192.168.1.21/mutillidae/index.php?page=register.php>
Attacked parameter: password
- Page: <http://192.168.1.21/bodgeit/login.jsp>
Attacked parameter: password
Cookie: JSESSIONID=9AAC0580FF9958EE4B5AF33FAAD75974
- Page: <http://192.168.1.21/WackoPicko/admin/index.php?page=login>
Attacked parameter: password
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: <http://192.168.1.21/WackoPicko/users/login.php>
Attacked parameter: password
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: <http://192.168.1.21/WackoPicko/passcheck.php>
Attacked parameter: password
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: <http://192.168.1.21/mutillidae/index.php?page=login.php>
Attacked parameter: password

Development / CSRF

High

Description: CSRF (or XSRF) attacks help an attacker to make the user performs requests without his consent

Remediation: Protect forms by adding a token with an unpredictable value and by checking this value when forms data are received

Priority: High

Methodology: black box

Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).

- Page: <http://192.168.1.21/bodgeit/basket.jsp>
Method: GET
Information : Form: '<form action="basket.jsp" method="post"></form>' is vulnerable





WORKGROUP\ORA9I (192.168.1.36)

Access control / Trivial account

Critical

Description: This Oracle database can be accessed using a trivial account (i.e. well known password, see the list of instances and accounts below).

Remediation: Change the passwords of these accounts or lock them.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

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

Patch mgt / Database patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
 Summary: Oracle Database Server and Application Server Ultra Search Component Unspecified Vulnerability
 Test script and information relative to this vulnerability: [802524](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-2008-0347](#)
- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
 Summary: Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
 Test script and information relative to this vulnerability: [802526](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-2006-0282](#), [CVE-2006-0291](#), [CVE-2006-0285](#), [CVE-2006-0290](#), [CVE-2006-0283](#), [CVE-2006-0286](#), [CVE-2006-0287](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server Multiple Unspecified Vulnerabilities - Jan 08
 Test script and information relative to this vulnerability: [802528](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-2008-0339](#), [CVE-2008-0340](#), [CVE-2008-0345](#), [CVE-2008-0341](#), [CVE-2008-0344](#), [CVE-2008-0343](#), [CVE-2008-0342](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server Multiple Unspecified Vulnerabilities
 Test script and information relative to this vulnerability: [802527](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [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](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server Multiple Vulnerabilities - Oct 06
 Test script and information relative to this vulnerability: [802520](#)
 Risk: 9.0 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
 References: [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](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server Multiple Unspecified Vulnerabilities - April 06



Test script and information relative to this vulnerability: [802538](#)
 Risk: 9.0 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
 References: [CVE-2006-1873](#) , [CVE-2006-1874](#) , [CVE-2006-1868](#) , [CVE-2006-1872](#) , [CVE-2006-1871](#)

- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server MDSYS.MD Buffer Overflows and Denial of Service Vulnerabilities
 Test script and information relative to this vulnerability: [802523](#)
 Risk: 8.5 (Impact: 9.2, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:N/I:C/A:C/).
 References: [CVE-2007-0272](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server 'RDBMS' component Denial of Service Vulnerability
 Test script and information relative to this vulnerability: [802539](#)
 Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
 References: [CVE-2007-5506](#)
- Summary: Oracle 9iAS SOAP Default Configuration Vulnerability
 Test script and information relative to this vulnerability: [11227](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2001-1371](#)
- Affected package: -ORACLE DATABASE
 Summary: Oracle Database Server Upgrade and Downgrade Component Multiple Vulnerabilities
 Test script and information relative to this vulnerability: [802519](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2007-2118](#) , [CVE-2007-2113](#)
- Affected package: -ORACLE DATABASE AND APPLICATION SERVER
 Summary: Oracle Database Server and Application Server Multiple Unspecified Vulnerabilities
 Test script and information relative to this vulnerability: [802525](#)
 Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
 References: [CVE-2006-0435](#)

Patch mgt / Windows patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Missing patch: [MS10-012](#)
 Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
 Test script and information relative to this vulnerability: [902269](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
- Missing patch: [MS09-001](#)
 Summary: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
 Test script and information relative to this vulnerability: [900233](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-2008-4835](#) , [CVE-2008-4114](#) , [CVE-2008-4834](#)
- Summary: SMB Registry : Windows Service Pack version
 Test script and information relative to this vulnerability: [10401](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
 References: [CVE-1999-0662](#)

Patch mgt / Web patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.



Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Affected package: -OPENSSL
Summary: OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability
Test script and information relative to this vulnerability: [100527](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-3245](#)
- Affected package: -OPENSSL
Summary: OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability
Test script and information relative to this vulnerability: [100668](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: [CVE-2010-0742](#)
- Summary: mod_ssl hook functions format string vulnerability
Test script and information relative to this vulnerability: [13651](#)
Risk: 7.5 (Impact: 6.4, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: [CVE-2004-0700](#)

Encryption / FTP service

High

Description: File transfer using FTP is not encrypted. The connection credentials and the data transferred can be caught and used by an evil individual.

Remediation: Consider using an encrypted file transport protocol (for instance, SFTP).

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 7.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

Configuration / Instance list available

High

Description: The Oracle database configuration enables to obtain the list of all the database instances.

Remediation: Migrate to a newer version (Oracle 10g minimum) and make sure the listener.ora file does not contain the line "LOCAL_OS_AUTHENTICATION_LISTENER = OFF".

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 7.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).

Information : [ORA9I]

Encryption / Weak SSL encryption

High

Description: The SSL server allows connections using weak ciphers (which key length is less than 128 bits), which could enable decoding connection credentials and data transferred in a timely manner.

Remediation: Restrict the list of encryption ciphers to only allow those which key length is 128 bits (at least).



Priority: High

Methodology: black box

Risk: 7.1 (Impact: 9.2, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:N).

Information : 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)

Access control / Trivial account

Critical

Description: This Microsoft SQL Server database can be accessed using a trivial administrator account (i.e. no password, or same password as login).

Remediation: Change administrator account password, or lock this account.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Information : SID : /1433 ([sa])

Configuration / Users list available

Critical

Description: The server version and configuration enables to obtain the list of its users.

Remediation: Migrate to a more recent operating system.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

Information : [Administrator, Guest, IUSR_VULNITSMB, IWAM_VULNITSMB, ToBeFound, TsInternetUser]

Access control / Open share folder

Critical

Description: The current configuration allows anyone to access the Windows shares listed below and to the files they contain.

Remediation: Restrict access to this Windows share to the authorized users only.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Information : [TESTSMB]

Configuration / SNMP community (write)

Critical

Description: A well-known SNMP community (see below) has write access on this server, which allows to remotely administrate the server (in particular, stop this server).

Remediation: Consider migrating to SNMP v3 in order to add authentication. Otherwise, change the community name or restrict the access to a list of allowed users.

Priority: Critical

Methodology: black box



Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Information : [private]

Patch mgt / Windows patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: black box

- Missing patch: MS10-012
Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
Test script and information relative to this vulnerability: 902269
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0022 , CVE-2010-0020 , CVE-2010-0021 , CVE-2010-0231
- Summary: IIS .IDA ISAPI filter applied
Test script and information relative to this vulnerability: 10695
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2001-0500
- Missing patch: MS11-035
Summary: Microsoft Windows WINS Remote Code Execution Vulnerability (2524426)
Test script and information relative to this vulnerability: 802260
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2011-1248

Configuration / RPC information leakage

Critical

Description: A RPC service provides to anyone many critical information on the system (with no need to be authenticated on the domain).

Remediation: Migrate to a more recent operating system.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

Information : 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 / Discard service

Critical

Description: The Discard service is open on this server. This service is unused today and should be closed.

Remediation: Close the Discard service, via /etc/inetd.conf on Unix, or via the registry ("EnableTcpDiscard" key) on Windows.

Priority: Critical



Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Configuration / SNMP community (read)

Critical

Description: An SNMP service in version 1 or 2 (without authentication) uses a well-known community name (see below) to provide many useful information on the system.

Remediation: Consider migrating to SNMP v3 in order to add authentication. Otherwise, change the community name or restrict the access to a list of allowed users.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:P/).

Information : 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.

Access control / Open mail relay

High

Description: This mail service allows anyone to send e-mail through it, which could enable masquerading (identity theft). Moreover, this mail server may be used by anonymous originators, in particular to relay spams.

Remediation: Apply the corrective patches if needed. Configure this server to accept and forward only the authorized messages (from authenticated senders).

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:C/A:N/).

Information : 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 / Web patch management

High

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.



Remediation: Install the patches provided by the editor.

Priority: High

Methodology: black box

- Summary: IIS XSS via 404 error
Test script and information relative to this vulnerability: [10936](#)
Risk: 7.6 (Impact: 6.6, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P).
References: [CVE-2002-0150](#) , [CVE-2002-0148](#)



VULNITLAB\SQL2K5 (192.168.1.54)

Patch mgt / Windows patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: white box

- Missing patch: MS11-042
Summary: Microsoft Distributed File System Remote Code Execution Vulnerabilities (2535512)
Test script and information relative to this vulnerability: 900288
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-1868 , CVE-2011-1869
- Missing patch: MS09-037
Summary: Vulnerabilities in Microsoft ATL Could Allow Remote Code Execution (973908)
Test script and information relative to this vulnerability: 101100
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2009-0901 , CVE-2009-2494 , CVE-2009-2493 , CVE-2008-0015
- Missing patch: MS08-076
Summary: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)
Test script and information relative to this vulnerability: 900060
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2008-3010 , CVE-2008-3009
- Missing patch: MS11-020
Summary: Microsoft Windows SMB Server Remote Code Execution Vulnerability (2508429)
Test script and information relative to this vulnerability: 900280
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0661
- Missing patch: MS10-020
Summary: Microsoft SMB Client Remote Code Execution Vulnerabilities (980232)
Test script and information relative to this vulnerability: 902156
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0476 , CVE-2010-0269 , CVE-2010-0270 , CVE-2010-0477 , CVE-2009-3676
- Missing patch: MS09-071
Summary: Microsoft Windows IAS Remote Code Execution Vulnerability (974318)
Test script and information relative to this vulnerability: 901065
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2505 , CVE-2009-3677
- Summary: Microsoft Windows2k3 Active Directory 'BROWSER ELECTION' Buffer Overflow Vulnerability
Test script and information relative to this vulnerability: 801598
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0654
- Missing patch: MS03-039
Summary: Microsoft RPC Interface Buffer Overrun (KB824146)
Test script and information relative to this vulnerability: 102015
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2003-0715 , CVE-2003-0528 , CVE-2003-0605
- Missing patch: ms08-007
Summary: Mini-Redirector Heap Overflow Vulnerability
Test script and information relative to this vulnerability: 90015
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2008-0080
- Missing patch: MS11-019
Summary: Microsoft SMB Client Remote Code Execution Vulnerabilities (2511455)
Test script and information relative to this vulnerability: 900279
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0660 , CVE-2011-0654
- Missing patch: MS11-043
Summary: Microsoft SMB Client Remote Code Execution Vulnerabilities (2536276)



- Test script and information relative to this vulnerability: [900287](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2011-1268](#)
- Missing patch: [MS08-067](#)
 Summary: Server Service Could Allow Remote Code Execution Vulnerability (958644)
 Test script and information relative to this vulnerability: [900055](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2008-4250](#)
 - Missing patch: [MS08-063](#)
 Summary: SMB Remote Code Execution Vulnerability (957095)
 Test script and information relative to this vulnerability: [900053](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2008-4038](#)
 - Missing patch: [MS10-054](#)
 Summary: Microsoft Windows SMB Code Execution and DoS Vulnerabilities (982214)
 Test script and information relative to this vulnerability: [901140](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2010-2550](#) , [CVE-2010-2552](#) , [CVE-2010-2551](#)
 - Missing patch: [MS09-001](#)
 Summary: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)
 Test script and information relative to this vulnerability: [900069](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2008-4835](#) , [CVE-2008-4114](#) , [CVE-2008-4834](#)
 - Missing patch: [MS10-012](#)
 Summary: Microsoft Windows SMB Server Multiple Vulnerabilities (971468)
 Test script and information relative to this vulnerability: [900230](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
 - Missing patch: [MS09-022](#)
 Summary: Vulnerabilities in Print Spooler Could Allow Remote Code Execution (961501)
 Test script and information relative to this vulnerability: [900667](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2009-0228](#) , [CVE-2009-0230](#) , [CVE-2009-0229](#)
 - Missing patch: [MS09-026](#)
 Summary: Vulnerability in RPC Could Allow Elevation of Privilege (970238)
 Test script and information relative to this vulnerability: [900668](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2009-0568](#)
 - Missing patch: [MS10-012](#)
 Summary: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
 Test script and information relative to this vulnerability: [902269](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2010-0022](#) , [CVE-2010-0020](#) , [CVE-2010-0021](#) , [CVE-2010-0231](#)
 - Missing patch: [MS09-034](#)
 Summary: Cumulative Security Update for Internet Explorer (972260)
 Test script and information relative to this vulnerability: [900906](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2009-1918](#) , [CVE-2009-1919](#) , [CVE-2009-1917](#)
 - Missing patch: [MS09-042](#)
 Summary: Telnet NTLM Credential Reflection Authentication Bypass Vulnerability (960859)
 Test script and information relative to this vulnerability: [900909](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2009-1930](#)
 - Summary: SMB Registry : Windows Service Pack version
 Test script and information relative to this vulnerability: [10401](#)
 Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-1999-0662](#)
 - Missing patch: [MS08-037](#)
 Summary: Vulnerabilities in DNS Could Allow Spoofing (953230)
 Test script and information relative to this vulnerability: [900005](#)
 Risk: 9.4 (Impact: 9.2, Exploitability: 10.0) CVSS : ([AV:N/AC:L/AU:N/C:N/I:C/A:C/](#)).
 References: [CVE-2008-1454](#) , [CVE-2008-1447](#)
 - Missing patch: [MS09-029](#)
 Summary: Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerabilities (961371)
 Test script and information relative to this vulnerability: [900689](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
 References: [CVE-2009-0231](#) , [CVE-2009-0232](#)
 - Missing patch: [MS10-001](#)



- Summary: Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerabilities (972270)
 Test script and information relative to this vulnerability: [901095](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-0018](#)
- Missing patch: [MS10-082](#)
 Summary: Microsoft Windows Media Player Remote Code Execution Vulnerability (2378111)
 Test script and information relative to this vulnerability: [901163](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-2745](#)
 - Missing patch: [MS10-035](#)
 Summary: Microsoft Internet Explorer Multiple Vulnerabilities (982381)
 Test script and information relative to this vulnerability: [902191](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-1261](#) , [CVE-2010-1259](#) , [CVE-2010-0255](#) , [CVE-2010-1262](#) , [CVE-2010-1260](#) , [CVE-2010-1257](#)
 - Missing patch: [MS07-042](#)
 Summary: Microsoft XML Core Services Remote Code Execution Vulnerability (936227)
 Test script and information relative to this vulnerability: [801715](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2007-2223](#)
 - Missing patch: [MS10-090](#)
 Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2416400)
 Test script and information relative to this vulnerability: [900262](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-3340](#) , [CVE-2010-3962](#) , [CVE-2010-3346](#) , [CVE-2010-3343](#) , [CVE-2010-3345](#) , [CVE-2010-3348](#) , [CVE-2010-3342](#)
 - Missing patch: [MS08-024](#)
 Summary: Microsoft Internet Explorer Data Stream Handling Remote Code Execution Vulnerability (947864)
 Test script and information relative to this vulnerability: [801488](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2008-1085](#)
 - Missing patch: [MS08-069](#)
 Summary: Microsoft XML Core Services Remote Code Execution Vulnerability (955218)
 Test script and information relative to this vulnerability: [900058](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2008-4033](#) , [CVE-2008-4029](#) , [CVE-2007-0099](#)
 - Missing patch: [MS10-053](#)
 Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2183461)
 Test script and information relative to this vulnerability: [901139](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-2557](#) , [CVE-2010-2558](#) , [CVE-2010-2560](#) , [CVE-2010-1258](#) , [CVE-2010-2556](#) , [CVE-2010-2559](#)
 - Missing patch: [MS11-003](#)
 Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2482017)
 Test script and information relative to this vulnerability: [901180](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2011-0035](#) , [CVE-2011-0038](#) , [CVE-2011-0036](#) , [CVE-2010-3971](#)
 - Missing patch: [MS08-001](#)
 Summary: Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (941644)
 Test script and information relative to this vulnerability: [801706](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2007-0069](#) , [CVE-2007-0066](#)
 - Missing patch: [MS10-062](#)
 Summary: MPEG-4 Codec Remote Code Execution Vulnerability (975558)
 Test script and information relative to this vulnerability: [900250](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2010-0818](#)
 - Missing patch: [MS07-050](#)
 Summary: Microsoft Windows Vector Markup Language Buffer Overflow (938127)
 Test script and information relative to this vulnerability: [102059](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2007-1749](#)
 - Missing patch: [MS09-011](#)
 Summary: Microsoft DirectShow Remote Code Execution Vulnerability (961373)
 Test script and information relative to this vulnerability: [900093](#)
 Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
 References: [CVE-2009-0084](#)



- Missing patch: MS08-010
Summary: Microsoft Internet Explorer HTML Rendering Remote Memory Corruption Vulnerability (944533)
Test script and information relative to this vulnerability: 801702
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2008-0076
- Missing patch: MS10-005
Summary: Microsoft Paint Remote Code Execution Vulnerability (978706)
Test script and information relative to this vulnerability: 902015
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0028
- Missing patch: MS10-013
Summary: Microsoft DirectShow Remote Code Execution Vulnerability (977935)
Test script and information relative to this vulnerability: 902117
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0250
- Missing patch: MS09-046
Summary: Microsoft DHTML Editing Component ActiveX Remote Code Execution Vulnerability (956844)
Test script and information relative to this vulnerability: 900837
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2519
- Missing patch: MS10-042
Summary: Microsoft Help and Support Center Remote Code Execution Vulnerability (2229593)
Test script and information relative to this vulnerability: 902080
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2010-1885
- Missing patch: MS10-007
Summary: Microsoft Windows Shell Handler Could Allow Remote Code Execution Vulnerability (975713)
Test script and information relative to this vulnerability: 900227
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0027
- Missing patch: MS09-052
Summary: Microsoft Windows Media Player ASF Heap Overflow Vulnerability (974112)
Test script and information relative to this vulnerability: 900879
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2527
- Missing patch: MS09-057
Summary: Microsoft Windows Indexing Service ActiveX Vulnerability (969059)
Test script and information relative to this vulnerability: 900881
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2507
- Missing patch: MS10-091
Summary: Microsoft Windows OpenType Compact Font Format Driver Privilege Escalation Vulnerability (2296199)
Test script and information relative to this vulnerability: 900263
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2010-3957 , CVE-2010-3956 , CVE-2010-3959
- Missing patch: MS09-047
Summary: sMicrosoft Windows Media Format Remote Code Execution Vulnerability (973812)
Test script and information relative to this vulnerability: 901012
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2499 , CVE-2009-2498
- Missing patch: MS09-061
Summary: Microsoft .NET Common Language Runtime Code Execution Vulnerability (974378)
Test script and information relative to this vulnerability: 900964
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2009-2497 , CVE-2009-0091 , CVE-2009-0090
- Missing patch: MS07-064
Summary: Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
Test script and information relative to this vulnerability: 801710
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: CVE-2007-3895 , CVE-2007-3901
- Summary: Microsoft Video ActiveX Control 'msvidctl.dll' BOF Vulnerability
Test script and information relative to this vulnerability: 800829
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).



- References: [CVE-2008-0020](#) , [CVE-2008-0015](#) -----
- Missing patch: [MS10-018](#)
Summary: Microsoft Internet Explorer Multiple Vulnerabilities (980182)
Test script and information relative to this vulnerability: [902155](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [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](#)
 - Missing patch: [MS11-038](#)
Summary: Microsoft Windows OLE Automation Remote Code Execution Vulnerability (2476490)
Test script and information relative to this vulnerability: [902377](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2011-0658](#)
 - Affected package: -INTERNET EXPLORER
Summary: Microsoft Internet Explorer HTML Form Value DoS Vulnerability
Test script and information relative to this vulnerability: [900303](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2009-0341](#)
 - Missing patch: [MS07-045](#)
Summary: Cumulative Security Update for Internet Explorer (937143)
Test script and information relative to this vulnerability: [102058](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2007-3041](#) , [CVE-2007-0943](#) , [CVE-2007-2216](#)
 - Missing patch: [MS09-045](#)
Summary: Microsoft JScript Scripting Engine Remote Code Execution Vulnerability (971961)
Test script and information relative to this vulnerability: [900929](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2009-1920](#)
 - Missing patch: [MS10-002](#)
Summary: Microsoft Internet Explorer Multiple Vulnerabilities (978207)
Test script and information relative to this vulnerability: [901097](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2010-0027](#) , [CVE-2009-4074](#) , [CVE-2010-0245](#) , [CVE-2010-0246](#) , [CVE-2010-0249](#) , [CVE-2010-0247](#) , [CVE-2010-0244](#) , [CVE-2010-0248](#)
 - Missing patch: [MS10-030](#)
Summary: Microsoft Outlook Express and Windows Mail Remote Code Execution Vulnerability (978542)
Test script and information relative to this vulnerability: [900241](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2010-0816](#)
 - Affected package: -WINDOWS MEDIA PLAYER
Summary: Microsoft Windows Media Player MID File Integer Overflow Vulnerability
Test script and information relative to this vulnerability: [900336](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2009-1331](#)
 - Missing patch: [MS09-065](#)
Summary: Microsoft Windows Kernel-Mode Drivers Multiple Vulnerabilities (969947)
Test script and information relative to this vulnerability: [900886](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2009-2514](#) , [CVE-2009-2513](#) , [CVE-2009-1127](#)
 - Missing patch: [MS07-068](#)
Summary: Vulnerability in Windows Media File Format Could Allow Remote Code Execution
Test script and information relative to this vulnerability: [801708](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2007-0064](#)
 - Missing patch: [MS10-096](#)
Summary: Microsoft Windows Address Book Remote Code Execution Vulnerability (2423089)
Test script and information relative to this vulnerability: [901169](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2010-3147](#)
 - Missing patch: [MS08-046](#)
Summary: Microsoft Windows Image Color Management System Code Execution Vulnerability (952954)
Test script and information relative to this vulnerability: [800023](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : ([AV:N/AC:M/AU:N/C:C/I:C/A:C/](#)).
References: [CVE-2008-2245](#)
 - Missing patch: [MS07-027](#)



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



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



- Test script and information relative to this vulnerability: [902300](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-2567](#)
- Missing patch: [MS09-054](#)
Summary: Microsoft Internet Explorer Multiple Code Execution Vulnerabilities (974455)
Test script and information relative to this vulnerability: [901041](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-2530](#) , [CVE-2009-1547](#) , [CVE-2009-2529](#) , [CVE-2009-2531](#)
 - Missing patch: [954157](#)
Summary: Microsoft Windows Indeo Codec Multiple Vulnerabilities
Test script and information relative to this vulnerability: [801090](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-4313](#) , [CVE-2009-4309](#) , [CVE-2009-4310](#) , [CVE-2009-4210](#) , [CVE-2009-4312](#) , [CVE-2009-4311](#)
 - Missing patch: [MS11-029](#)
Summary: Microsoft GDI+ Remote Code Execution Vulnerability (2489979)
Test script and information relative to this vulnerability: [902365](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2011-0041](#)
 - Missing patch: [MS09-014](#)
Summary: Microsoft Internet Explorer Remote Code Execution Vulnerability (963027)
Test script and information relative to this vulnerability: [900328](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-0554](#) , [CVE-2009-0553](#) , [CVE-2009-0550](#) , [CVE-2009-0552](#) , [CVE-2008-2540](#) , [CVE-2009-0551](#)
 - Missing patch: [MS11-006](#)
Summary: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)
Test script and information relative to this vulnerability: [902334](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-3970](#)
 - Missing patch: [MS07-017](#)
Summary: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
Test script and information relative to this vulnerability: [801720](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-1215](#) , [CVE-2007-1211](#) , [CVE-2007-0038](#) , [CVE-2007-1213](#) , [CVE-2007-1212](#)
 - Missing patch: [MS08-045](#)
Summary: Cumulative Security Update for Internet Explorer (953838)
Test script and information relative to this vulnerability: [900030](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2008-2257](#) , [CVE-2008-2258](#) , [CVE-2008-2254](#) , [CVE-2008-2259](#) , [CVE-2008-2256](#) , [CVE-2008-2255](#)
 - Missing patch: [MS08-068](#)
Summary: SMB Could Allow Remote Code Execution Vulnerability (957097)
Test script and information relative to this vulnerability: [900057](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2008-4037](#)
 - Missing patch: [MS10-071](#)
Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2360131)
Test script and information relative to this vulnerability: [901162](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [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](#)
 - Missing patch: [MS09-006](#)
Summary: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)
Test script and information relative to this vulnerability: [900086](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-0082](#) , [CVE-2009-0083](#) , [CVE-2009-0081](#)
 - Missing patch: [MS10-046](#)
Summary: Microsoft Windows Shell Remote Code Execution Vulnerability (2286198)
Test script and information relative to this vulnerability: [902226](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-2568](#)
 - Missing patch: [MS08-058](#)
Summary: Cumulative Security Update for Internet Explorer (956390)
Test script and information relative to this vulnerability: [900054](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).



- References: [CVE-2008-3474](#) , [CVE-2008-3476](#) , [CVE-2008-3473](#) , [CVE-2008-3475](#) , [CVE-2008-3472](#) , [CVE-2008-2947](#)
- Missing patch: [MS07-034](#)
Summary: Microsoft Outlook Express/Windows Mail MHTML URI Handler Information Disclosure Vulnerability (929123)
Test script and information relative to this vulnerability: [801716](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2006-2111](#) , [CVE-2007-2225](#) , [CVE-2007-2225](#) , [CVE-2007-1658](#)
 - Missing patch: [MS11-050](#)
Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2530548)
Test script and information relative to this vulnerability: [902443](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [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](#)
 - Missing patch: [MS11-057](#)
Summary: Microsoft Internet Explorer Multiple Vulnerabilities (2559049)
Test script and information relative to this vulnerability: [902613](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2011-1257](#) , [CVE-2011-1962](#) , [CVE-2011-1963](#) , [CVE-2011-1960](#) , [CVE-2011-1961](#) , [CVE-2011-1964](#) , [CVE-2011-2383](#)
 - Summary: MS Internet Explorer 'Style' Object Remote Code Execution Vulnerability
Test script and information relative to this vulnerability: [800727](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-3674](#) , [CVE-2009-3671](#) , [CVE-2009-3673](#) , [CVE-2009-3672](#) , [CVE-2009-2493](#)
 - Missing patch: [MS09-051](#)
Summary: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)
Test script and information relative to this vulnerability: [901039](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-2525](#) , [CVE-2009-0555](#)
 - Missing patch: [MS07-004](#)
Summary: Microsoft Windows Vector Markup Language Vulnerabilities (929969)
Test script and information relative to this vulnerability: [102053](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-0024](#)
 - Missing patch: [MS09-038](#)
Summary: Microsoft Windows AVI Media File Parsing Vulnerabilities (971557)
Test script and information relative to this vulnerability: [900907](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-1545](#) , [CVE-2009-1546](#)
 - Missing patch: [ms08-028](#)
Summary: Windows Vulnerability in Microsoft Jet Database Engine
Test script and information relative to this vulnerability: [90024](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-6026](#)
 - Missing patch: [ms08-078](#)
Summary: Vulnerability in Internet Explorer Could Allow Remote Code Execution (960714)
Test script and information relative to this vulnerability: [900066](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2008-4844](#)
 - Missing patch: [MS09-019](#)
Summary: Cumulative Security Update for Internet Explorer (969897)
Test script and information relative to this vulnerability: [900364](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-3091](#) , [CVE-2009-1528](#) , [CVE-2009-1529](#) , [CVE-2009-1531](#) , [CVE-2009-1140](#) , [CVE-2009-1532](#) , [CVE-2009-1530](#) , [CVE-2009-1141](#)
 - Missing patch: [MS07-069](#)
Summary: Microsoft Internet Explorer mshtml.dll Remote Memory Corruption Vulnerability (942615)
Test script and information relative to this vulnerability: [801707](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-5344](#) , [CVE-2007-3903](#) , [CVE-2007-3902](#) , [CVE-2007-5347](#)
 - Summary: Microsoft Windows Progman Group Converter Insecure Library Loading Vulnerability
Test script and information relative to this vulnerability: [801456](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-3139](#)



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



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



- Affected package: -INTERNET EXPLORER
Summary: Microsoft Internet Explorer Denial Of Service Vulnerability - July09
Test script and information relative to this vulnerability: 800669
Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).
References: CVE-2009-2536 , CVE-2009-1692
- Missing patch: MS08-061
Summary: Windows Kernel Elevation of Privilege Vulnerability (954211)
Test script and information relative to this vulnerability: 900051
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2008-2250 , CVE-2008-2251 , CVE-2008-2252
- Missing patch: MS08-064
Summary: Virtual Address Descriptor Manipulation Elevation of Privilege Vulnerability (956841)
Test script and information relative to this vulnerability: 900225
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2008-4036
- Summary: Microsoft Windows Server 2003 OpenType Font Engine DoS Vulnerability
Test script and information relative to this vulnerability: 800687
Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).
References: CVE-2009-3020
- Missing patch: MS11-034
Summary: Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2506223)
Test script and information relative to this vulnerability: 900283
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: 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
- Missing patch: MS11-062
Summary: MS Windows Remote Access Service NDISTAPI Driver Privilege Elevation Vulnerability (2566454)
Test script and information relative to this vulnerability: 900298
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-1974
- Missing patch: MS11-013
Summary: Microsoft Kerberos Privilege Escalation Vulnerabilities (2496930)
Test script and information relative to this vulnerability: 902288
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0043 , CVE-2011-0091
- Missing patch: MS11-056
Summary: Microsoft Windows CSRSS Privilege Escalation Vulnerabilities (2507938)
Test script and information relative to this vulnerability: 902609
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-1283 , CVE-2011-1284 , CVE-2011-1282 , CVE-2011-1870 , CVE-2011-1281
- Missing patch: MS08-025
Summary: Microsoft Windows Kernel Usermode Callback Local Privilege Elevation Vulnerability (941693)
Test script and information relative to this vulnerability: 801487
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2008-1084
- Missing patch: MS09-007
Summary: Vulnerability in SChannel Could Allow Spoofing (960225)
Test script and information relative to this vulnerability: 900087
Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:C/A:N/).
References: CVE-2009-0085
- Missing patch: MS10-084
Summary: Windows Local Procedure Call Privilege Elevation Vulnerability (2360937)
Test script and information relative to this vulnerability: 902322
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-3222
- Missing patch: MS07-017
Summary: Microsoft Windows GDI Multiple Vulnerabilities (925902)
Test script and information relative to this vulnerability: 102055
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2007-1215 , CVE-2006-5586 , CVE-2007-1211 , CVE-2006-5758 , CVE-



- 2007-1213 , CVE-2007-1212
- Missing patch: MS10-078
Summary: OpenType Font (OTF) Format Driver Privilege Elevation Vulnerabilities (2279986)
Test script and information relative to this vulnerability: 902320
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-2740 , CVE-2010-2741
 - Summary: Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability
Test script and information relative to this vulnerability: 800442
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0232
 - Missing patch: MS11-065
Summary: Microsoft Remote Desktop Protocol Denial of Service Vulnerability (2570222)
Test script and information relative to this vulnerability: 902708
Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).
References: CVE-2011-1968
 - Missing patch: MS11-011
Summary: Microsoft Windows Kernel Elevation of Privilege Vulnerability (2393802)
Test script and information relative to this vulnerability: 902337
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0045 , CVE-2010-4398
 - Missing patch: MS09-025
Summary: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)
Test script and information relative to this vulnerability: 900669
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2009-1124 , CVE-2009-1125 , CVE-2009-1126 , CVE-2009-1123
 - Missing patch: MS10-073
Summary: Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (981957)
Test script and information relative to this vulnerability: 902323
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-2549 , CVE-2010-2743 , CVE-2010-2744
 - Missing patch: MS11-014
Summary: Microsoft Windows LSASS Privilege Escalation Vulnerability (2478960)
Test script and information relative to this vulnerability: 902289
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0039
 - Summary: Microsoft Windows win32k.sys Driver 'CreateDIBPalette()' BOF Vulnerability
Test script and information relative to this vulnerability: 902256
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-2739
 - Missing patch: MS11-054
Summary: Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2555917)
Test script and information relative to this vulnerability: 902538
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: 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
 - Missing patch: MS11-012
Summary: Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2479628)
Test script and information relative to this vulnerability: 901182
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-0088 , CVE-2011-0090 , CVE-2011-0086 , CVE-2011-0089 , CVE-2011-0087
 - Missing patch: MS10-015
Summary: Microsoft Windows Kernel Could Allow Elevation of Privilege (977165)
Test script and information relative to this vulnerability: 900740
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2010-0232 , CVE-2010-0233
 - Missing patch: MS11-046
Summary: MS Windows Ancillary Function Driver Privilege Elevation Vulnerability
Test script and information relative to this vulnerability: 902442
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2011-1249
 - Missing patch: MS07-021
Summary: Microsoft Windows CSRSS CSRFinalizeContext Local Privilege Escalation Vulnerability (930178)
Test script and information relative to this vulnerability: 801719
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: CVE-2007-1209 , CVE-2006-6696



Patch mgt / Database patch management	Major
<p>Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.</p> <p>Remediation: Install the patches provided by the editor.</p> <p>Priority: Major</p> <p>Methodology: white box</p> <ul style="list-style-type: none">• Missing patch: <u>MS08-040</u> Summary: MS SQL Server Elevation of Privilege Vulnerabilities (941203) Test script and information relative to this vulnerability: <u>800105</u> Risk: 9.0 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/). References: <u>CVE-2008-0085</u> , <u>CVE-2008-0086</u> , <u>CVE-2008-0106</u> , <u>CVE-2008-0107</u>	
Configuration / Instance list available	High
<p>Description: The Microsoft SQL Server version and configuration enable to obtain the list of all the database instances.</p> <p>Remediation: Stop the 'SQL Server Browser' service. Otherwise, restrict access to the 1434/UDP port to authorized users only.</p> <p>Priority: High</p> <p>Methodology: black box</p> <p>Risk: 7.8 (Impact: 7.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:P/A:N/).</p> <p>Information : TOBEFOUND (9.00.1399.06)</p>	



VULNITLAB\WINXP (192.168.1.84)

Patch mgt / Windows patch management

Critical

Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.

Remediation: Install the patches provided by the editor.

Priority: Critical

Methodology: white box

- Summary: Microsoft Windows XP SP3 denial of service vulnerability
Test script and information relative to this vulnerability: [800504](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-0119](#)
- Affected package: -WINDOWS AND SERVICE PACK
Summary: Microsoft GDIPlus PNG Infinite Loop Vulnerability
Test script and information relative to this vulnerability: [800700](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:N/A:C/).
References: [CVE-2009-1511](#)
- Summary: SMB Registry : Windows Service Pack version
Test script and information relative to this vulnerability: [10401](#)
Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-1999-0662](#)
- Summary: Microsoft Windows Address Book Insecure Library Loading Vulnerability
Test script and information relative to this vulnerability: [801457](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-3143](#) , [CVE-2010-3147](#)
- Affected package: -WINDOWS MEDIA PLAYER
Summary: Microsoft Windows Media Player MID File Integer Overflow Vulnerability
Test script and information relative to this vulnerability: [900336](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-1331](#)
- Affected package: -INTERNET EXPLORER
Summary: MS Internet Explorer Remote Code Execution Vulnerability (981374)
Test script and information relative to this vulnerability: [800176](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-0806](#)
- Missing patch: [MS09-028](#)
Summary: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution
Test script and information relative to this vulnerability: [900097](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-1537](#)
- Affected package: -INTERNET EXPLORER
Summary: Microsoft Internet Explorer Remote Code Execution Vulnerability (979352)
Test script and information relative to this vulnerability: [800429](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-0249](#)
- Affected package: -INTERNET EXPLORER
Summary: Microsoft Internet Explorer Denial Of Service Vulnerability - July09
Test script and information relative to this vulnerability: [800669](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:N/A:C/).
References: [CVE-2009-2536](#) , [CVE-2009-1692](#)
- Missing patch: [954157](#)
Summary: Microsoft Windows Indeo Codec Multiple Vulnerabilities
Test script and information relative to this vulnerability: [801090](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-4313](#) , [CVE-2009-4309](#) , [CVE-2009-4310](#) , [CVE-2009-4210](#) , [CVE-2009-4312](#) , [CVE-2009-4311](#)
- Summary: Microsoft Windows TrueType Font Parsing Privilege Elevation Vulnerability
Test script and information relative to this vulnerability: [802500](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2011-3402](#)
- Summary: Adobe Flash Player 9.0.115.0 and earlier vulnerability (Win)
Test script and information relative to this vulnerability: [90019](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).



- References: [CVE-2007-5275](#) , [CVE-2008-1655](#) , [CVE-2007-6637](#) , [CVE-2007-6243](#) , [CVE-2007-6019](#) , [CVE-2008-1654](#)
- Summary: MS Internet Explorer 'Style' Object Remote Code Execution Vulnerability
Test script and information relative to this vulnerability: [800727](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2009-3674](#) , [CVE-2009-3671](#) , [CVE-2009-3673](#) , [CVE-2009-3672](#) , [CVE-2009-2493](#)
 - Missing patch: [MS09-019](#)
Summary: Cumulative Security Update for Internet Explorer (969897)
Test script and information relative to this vulnerability: [900364](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2007-3091](#) , [CVE-2009-1528](#) , [CVE-2009-1529](#) , [CVE-2009-1531](#) , [CVE-2009-1140](#) , [CVE-2009-1532](#) , [CVE-2009-1530](#) , [CVE-2009-1141](#)
 - Summary: Microsoft Windows Progman Group Converter Insecure Library Loading Vulnerability
Test script and information relative to this vulnerability: [801456](#)
Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-3139](#)
 - Missing patch: [MS08-062](#)
Summary: Windows Internet Printing Service Allow Remote Code Execution Vulnerability (953155)
Test script and information relative to this vulnerability: [900052](#)
Risk: 9.0 (Impact: 10.0, Exploitability: 8.0) CVSS : (AV:N/AC:L/AU:S/C:C/I:C/A:C/).
References: [CVE-2008-1446](#)
 - Summary: Windows Messenger is installed
Test script and information relative to this vulnerability: [11429](#)
Risk: 8.8 (Impact: 8.3, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).
References: [CVE-2002-0228](#) , [CVE-1999-1484](#) , [CVE-2002-0472](#)
 - Missing patch: [981169](#)
Summary: MS Internet Explorer 'VBScript' Remote Code Execution Vulnerability
Test script and information relative to this vulnerability: [800482](#)
Risk: 7.6 (Impact: 10.0, Exploitability: 4.9) CVSS : (AV:N/AC:H/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-0483](#)
 - Summary: Windows XP 'SPI_GETDESKWALLPAPER' DoS Vulnerability
Test script and information relative to this vulnerability: [900724](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:N/I:N/A:C/).
References: [CVE-2009-1808](#)
 - Affected package: -MICROSOFT EXPLORER
Summary: Microsoft Explorer HTTPS Sessions Multiple Vulnerabilities (Windows)
Test script and information relative to this vulnerability: [802140](#)
Risk: 7.1 (Impact: 6.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:P/A:P/).
References: [CVE-2008-7295](#)
 - Summary: Microsoft Windows GP Trap Handler Privilege Escalation Vulnerability
Test script and information relative to this vulnerability: [800442](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-0232](#)
 - Summary: Microsoft Windows win32k.sys Driver 'CreateDIBPalette()' BOF Vulnerability
Test script and information relative to this vulnerability: [902256](#)
Risk: 7.1 (Impact: 10.0, Exploitability: 3.9) CVSS : (AV:L/AC:L/AU:N/C:C/I:C/A:C/).
References: [CVE-2010-2739](#)

Configuration / Software disabled

Major

Description: Security software is disabled

Remediation: Enable the product

Priority: Major

Methodology: white box

Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

Information : WindowsFirewall - Domain profile



Configuration / Passwords complexity requirements disable	Major
<p>Description: Passwords complexity requirements prevents users to define easy passwords</p> <p>Remediation: Enable passwords complexity requirements</p> <p>Priority: Major</p> <p>Methodology: white box</p> <p>Risk: 8.8 (Impact: 8.3, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).</p>	
Configuration / Minimum password length too low	Major
<p>Description: A password too short increases probability of a successful brute-force attack</p> <p>Remediation: Increase minimum password length (at least 6 characters)</p> <p>Priority: Major</p> <p>Methodology: white box</p> <p>Risk: 8.8 (Impact: 8.3, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:P/A:P/).</p> <p>Information : 3</p>	
Configuration / Local user account enabled	Major
<p>Description: Local account enabled on a machine member of a domain</p> <p>Remediation: Disable local accounts</p> <p>Priority: Major</p> <p>Methodology: white box</p> <p>Risk: 8.1 (Impact: 8.3, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).</p> <p>Information : Vulnit</p>	
Configuration / Password never expires	Major
<p>Description: The password never expires, which increases probability of a successful brute-force attack</p> <p>Remediation: Remove the option which allows non-expiring password</p> <p>Priority: Major</p> <p>Methodology: white box</p> <p>Risk: 8.1 (Impact: 8.3, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:P/).</p> <p>Information : Administrateur, Vulnit</p>	



Annexes

Annex A: Glossary

- **Target** - generic term which means server, desktop, workstation, printer, router or any other device accessible on the network.
- **Patch** - update fixing one or more vulnerabilities. Patches concern operating systems, databases, softwares, or packets (Unix).
- **CVSS** - Common Vulnerability Scoring System. This is an assessment standard of the severity of computer system security vulnerabilities. The Base metric is displayed as a 6-letter vector following each risk.
- **DBMS** - DataBase Management System.
- **Exploitability** - easiness to exploit a vulnerability. A higher exploitability indicates that the vulnerability requires less skills to be exploited, so a threat may more likely occur.
- **Function** - the control function determines the roots of a vulnerability. For instance, an SQL injection is caused by a development mistake. A trivial password comes from a wrong access control parameterization. The configuration of a service may also lead to information leakage.
- **Impact** - potential effect on the service availability, the confidentiality or the integrity of the data stored on a target.
- **DNS name** - Domaine Name Server. A name obtained by reverse resolution from the DNS server.
- **Netbios name** - Name of a target belonging to a Windows domain or workgroup.
- **Object** - the system concerned by the vulnerability: operating system (including the applications installed on the OS), DBMS, web servers/sites or network.
- **Priority** - The 3 levels (Critical, Major and High) suggested in this report facilitate the identification of the most critical vulnerabilities in order to address them first.
Note: all the vulnerabilities mentioned in this report are high-risk issues (CVSS greater than 7) and thus, should all be addressed.
- **Risk** - potentiel risk of a threat exploiting the vulnerability. The final risk of a vulnerability should also consider the value of the targeted asset (i.e. the criticity of the information stored in this target or the operational dependancy to the services provided by this target) and the controls that could mitigate the risk (audit logs, contingency plan, etc).
The risk computation is explained in this document (in the Base metric chapter).
- **Vulnerability** - weakness which allows an attacker to reduce a system's information assurance (in terms of service availability, integrity or confidentiality of the information stored on the targeted device).



Annex B: Auditing tools

- **Aircrack** is a set of auditing tools allowing to analyse the security of wifi access points. Author and maintainer: Thomas d'Otreppe.
- **CSRF Scanner** is a tool designed to find CSRF (Cross-Site Request Forgery) security flaws on forms.. Author et maintainer: VulnIT.
- **db2getprofile** (part of the db2utils suite) gets the access profile to DB2 database and particularly lists the instances and databases. Author and maintainer: Patrik Karlsson.
- **dhcping** is a DHCP and BOOTP scanner. Author et maintainer: Edwin Groothuis.
- **dig** - provided within the dnsutils package - allows to request a DNS server to get the list of the nameservers by DNS zone transfer. Author and maintainer: Internet Systems Consortium, Inc (ISC).
- **flasm** disassembles SWF menus in order to extract the links redirecting to other webpages. Author and maintainer: Ben Schleimer.
- **Medusa** allows to test connexion ID on lots of services (FTP, SSH, SNMP, SMTP...). Author and maintainer: JoMo-Kun.
- **mit-krb5** implements under unix the kerberos protocol used for the domain authentication (when the domain is managed by an Active Directory starting from Windows 2003). Author and maintainer: Massachusetts Institute of Technology.
- **MSSQLScan** allows to get some informations on Microsoft SQL Server database. Author and maintainer: Patrik Karlsson.
- **nbtscan** includes the same features as windows 'nbtstat' command (listing all open Netbios services). Author and maintainer: Stephen Friedl.
- **netcat** allows to establish network connexions and adds a lot of useful features to telnet. Author and maintainer: Giovanni Giacobbi.
- **Nmap**, the famous ports scanner used to detect running services on targets. Auteur et mainteneur: Gordon Lyon.
- **OpenVAS** integrates several thousands of tests upon patch management: OS, applications, DBMS, etc. Author and maintainer: OpenVAS team.
- **rpcclient** allows to acces to "named pipe" and to execute MS RPC commands. It's part of the Samba suite. Author and maintainer: Samba team.
- **opwg** (part of the Oracle Auditing Tools suite) attacks an Oracle database using a dictionary. Author and maintainer: Patrik Karlsson.
- **SidGuesser** allows to discover Oracle instances when they are transmitted by listener (attacking using a dictionary). Author and maintainer: Patrik Karlsson.
- **snmpwalk** provided within the net-snmp package allows to browse informations given by SNMP protocol. Author and maintainer: Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) includes smbdumpusers tool allowing to list the users of Windows NT/2000. Author and maintainer: Patrik Karlsson.
- **smbclient** is an equivalent to 'net use' from Windows and allows to get informations on Windows sharing. Author and maintainer: Samba team.
- **sqlmap** is an open source penetration testing tool that automates the process of detecting SQL injection flaws. Author and maintainer: Bernardo Damele.
- **sslscan** determines which cryptographic algorithms is in use on a SSL server (basically in the case of an https webapplication). Author and maintainer: Ian Ventura-Whiting.
- **tnscmd10g** allows to list the instances of the Oracle database (including 10g and 11g versions). Author: James W. Abendschan, Maintainer: Saez Scheihing.
- **WhatWeb** identifies content management systems (CMS), blogging platforms, stats/analytics packages, javascript libraries, servers and more. Author and maintainer: Brendan Coles.
- **wdiff** is a front end to diff for comparing files on a word per word basis. Author and maintainer: Denver Gingerich.
- **XSS Scanner** is an open-source tool designed to find XSS (Cross-Site Scripting) injections. Author et maintainer: VulnIT.

Annex C: Report generation

- **The eZ Components library** allows to generate all the figures inside this report. Author and maintainer: eZ Systems.
- **PostgreSQL** is a relational database management system (RDBMS). Author and maintainer: PostgreSQL Global Development
- **wkhtmltopdf** (read: WebKit HTML to PDF) combines the strength of the XHTML/CSS Webkit engine (used by Chrome and Safari for example) and its PDF library. Author and maintainer: Jakob Truelsen.



Group.



Legal notice

In accordance with the LCEN Act of 22 June 2004, the VulnIT product is exclusively made available for legitimate users and businesses whom their mission is to perform security audits. By accepting the VulnIT agreement license, the user agrees to abide by the Godfrain act of January 6, 1988 punishing unauthorized intrusions into a computer system.

Copyright statement

The name VulnIT, logo and all graphical related material in this report are, unless otherwise stated, the property of VulnIT. Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.
