Vulnerabilities
MANAGEMENT

Scan Task Vulnerabilities Report

Scan:	QuanTriTT1_2_sang_300818
Submit by:	admin
Generated Time:	Oct. 2, 2018, 2 p.m.

Table Of Contents

Scan Task Detailed Information

Information

Scan Task:		QuanTriTT1_2_sang_300818	
Create by:		admin	
Project:	Administrative Machines	**Processed:**	No
Start Time:	Aug. 30, 2018, 4:30 a.m.	**Finished Time:**	Aug. 30, 2018, 4:57 a.m.
Created Date:	Sept. 10, 2018, 3:30 a.m.	**Updated Date:**	Sept. 24, 2018, 2:48 a.m.

Description:

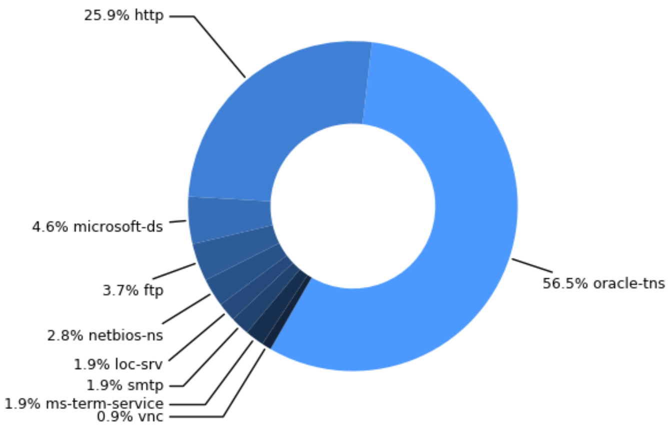
NA#

Vulnerabilities

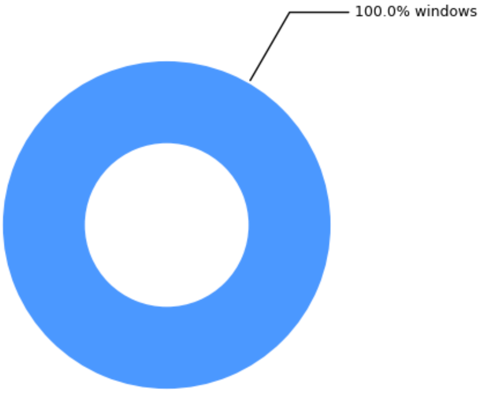
Overview

In this section, this report contains overview information that includes statistics by services (in graph-1), OS (in graph-2) and current categorized vulnerabilities (in graph-3) into groups:

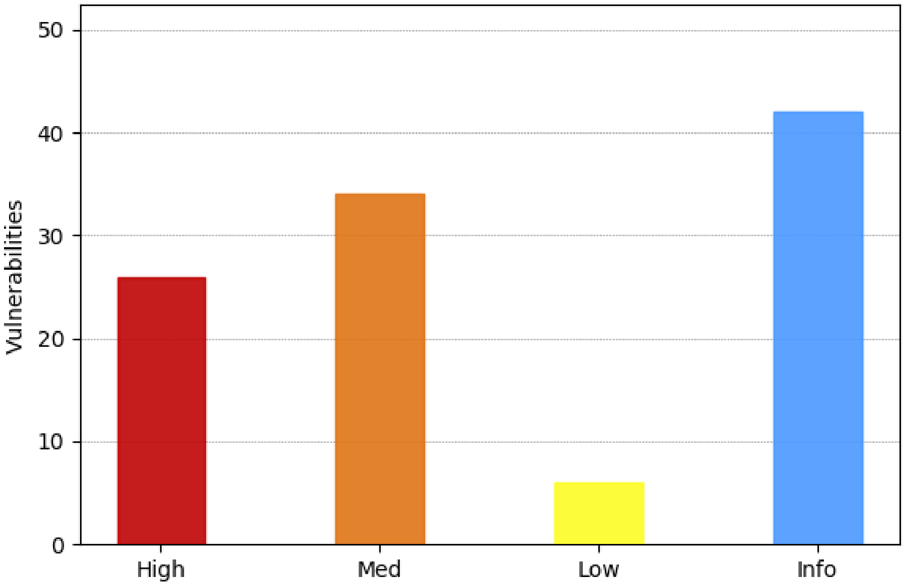
- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection.
- **Low Risk** - The vulnerability discovered on the system provides enticement data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker gaining some form of access to the machine over a remote connection.
- **Informational Risk** - A finding on the system that provides data to an attacker that is of lesser value to an attacker than the enticement data provided by a low risk vulnerability.



Graph 1: Vulnerabilities statistic by services



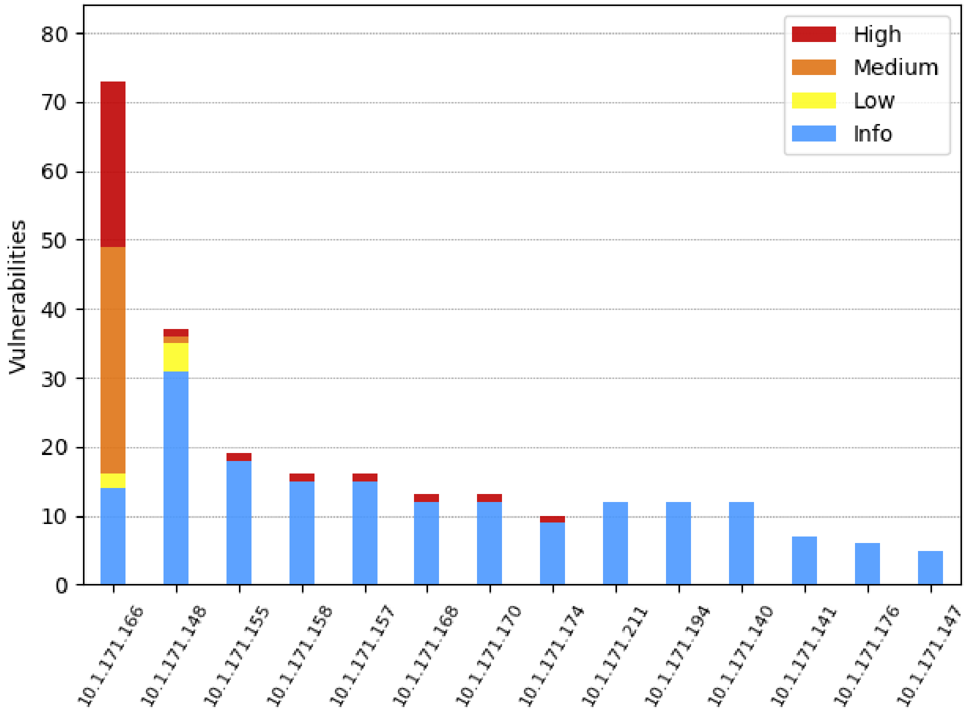
Graph 2: Vulnerabilities statistic by OS



Graph 3: Vulnerabilities statistic

Vulnerabilities in Scan Task

In this section, the report contains scan brief information of vulnerabilities that were discovered by this scan task.



Graph 4: Vulnerabilities of scanned hosts

Scan Result:

Hostname	Ip Address	Vulnerabilities			
		High	Med	Low	Info
HO-CNTT-TT2-056	10.1.171.166	24	33	2	14
HO-CNTT-TT2-029	10.1.171.148	1	1	4	31
HO-CNTT-TT2-035	10.1.171.155	1	0	0	18
HO-CNTT-TT2-014	10.1.171.158	1	0	0	15
HO-CNTT-TT2-037	10.1.171.157	1	0	0	15
HO-CNTT-TT2-019	10.1.171.168	1	0	0	12
HO-CNTT-TT2-067	10.1.171.170	1	0	0	12
HO-CNTT-TT2-025	10.1.171.174	1	0	0	9
HO-CNTT-TT2-030	10.1.171.211	0	0	0	12
HO-CNTT-TT2-044	10.1.171.194	0	0	0	12
HO-CNTT-TT2-131	10.1.171.140	0	0	0	12
HO-CNTT-TT2-005	10.1.171.141	0	0	0	7
HO-CNTT-TT2-054	10.1.171.176	0	0	0	6
HO-CNTT-TT2-016	10.1.171.147	0	0	0	5

Table 1: Vulnerabilities in Scan Task

Vulnerabilities by Host

In this section, Discovered Vulnerabilities are grouped by host.

HO-CNTT-TT2-131 - 10.1.171.140

Vulnerabilities	Service	Level Risk
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-016 - 10.1.171.147

Vulnerabilities	Service	Level Risk
LSASS RPC Interface Detected	loc-srv	0.0
VNC Server Detected	vnc	0.0
Web Server Broken Links Detected	http	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
Hidden WWW Server Name Detected	http	0.0

HO-CNTT-TT2-035 - 10.1.171.155

Vulnerabilities	Service	Level Risk
Oracle Database Server TNS Listener Poison Attack Remote Code Execution	oracle-tns	9.0
Microsoft IIS Host Name Setting Enumerated	http	0.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Anonymous Access Enabled	http	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft ASP.NET HTTP Handlers Enumeration	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Microsoft ASP.NET State Service Detected	http	0.0
Hidden WWW Server Name Detected	http	0.0
Microsoft Windows IIS ASP.NET Version Detection	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft IIS Server Extensions Enumerated	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-056 - 10.1.171.166

Vulnerabilities	Service	Level Risk
Oracle Database Listener Component Information Disclosure Vulnerability	oracle-tns	10.0
Oracle Database April 2012 Critical Patch Update	oracle-tns	9.0

Vulnerabilities	Service	Level Risk
Oracle Database Server January 2013 Critical Patch Update	oracle-tns	9.0
Oracle Database October 2011 Critical Patch Update	oracle-tns	9.0
Oracle Database Server TNS Listener Poison Attack Remote Code Execution	oracle-tns	9.0
Oracle Database Critical Patch Update April 2013	oracle-tns	9.0
Oracle Database Server Oracle Text Privilege Escalation	oracle-tns	9.0
Oracle Database Server Listener Oracle Net Remote Authentication Bypass Vulnerability (CVE-2010-0911)	oracle-tns	8.0
Oracle Database October 2010 Critical Patch Update	oracle-tns	8.0
Oracle Database October 2009 Critical Patch Update	oracle-tns	8.0
Oracle Database April 2010 Critical Patch Update	oracle-tns	8.0
Oracle Database January 2010 Critical Patch Update	oracle-tns	8.0
Oracle Database Core RDBMS Component Vulnerability (CVE-2010-0860)	oracle-tns	8.0
Oracle Database July 2010 Critical Patch Update	oracle-tns	8.0
Oracle Database Critical Patch Update July 2013	oracle-tns	8.0
Oracle Database July 2012 Critical Patch Update	oracle-tns	7.0
Oracle Database Server Change Data Capture GSS-API Library Denial Of Service (CVE-2010-1321)	oracle-tns	7.0
Oracle Database Server Net Foundation Layer Remote Authentication Bypass Vulnerability (CVE-2010-0903)	oracle-tns	7.0
Oracle Database July 2011 Critical Patch Update	oracle-tns	7.0
Oracle Database and Enterprise Manager Grid Control Remote Code Execution	oracle-tns	7.0
Oracle Database Server Java SecurityManager Remote Code Execution (CVE-2010-2419)	oracle-tns	7.0
Oracle Database Server OLAP Information Disclosure (CVE-2010-2412)	oracle-tns	7.0
Oracle Database Server October 2012 Critical Patch Update	oracle-tns	7.0
Oracle Database CTXSYS.CONTEXT Privilege Escalation Vulnerability	oracle-tns	7.0
Oracle Database January 2011 Critical Patch Update	oracle-tns	6.0
Oracle Database April 2011 Critical Patch Update	oracle-tns	6.0

Vulnerabilities	Service	Level Risk
Oracle Database Server Core RDBMS Privilege Escalation	oracle-tns	5.0
Oracle Database Vault Remote Security Bypass	oracle-tns	5.0
Oracle Database Scheduler Agent Information Disclosure	oracle-tns	5.0
Oracle Database Data Pump Component Vulnerability (CVE-2009-3411)	oracle-tns	5.0
Oracle Database Vault Remote Security Bypass I	oracle-tns	5.0
Oracle Database Cluster Verify Utility Privilege Escalation	oracle-tns	5.0
Oracle Database Server Listener Oracle Net Denial Of Service	oracle-tns	5.0
Oracle Database JavaVM Component Vulnerability (CVE-2010-0867)	oracle-tns	5.0
Oracle Database DBMS_JAVA.SET_OUTPUT_TO_JAVA Privilege Escalation Vulnerability	oracle-tns	5.0
Oracle Database Server Core RDBMS Create Session Information Disclosure	oracle-tns	5.0
Oracle Database Vault Privilege Escalation	oracle-tns	5.0
Oracle Database JavaVM Component Vulnerability (CVE-2010-0866)	oracle-tns	5.0
Oracle Database January 2012 Critical Patch Update	oracle-tns	5.0
Oracle Database UIX Security Bypass	oracle-tns	5.0
Oracle Fusion Middleware Help Security Bypass	oracle-tns	5.0
Oracle Database Server Job Queue Remote Code Execution (CVE-2010-2411)	oracle-tns	5.0
Oracle Database Network Foundation Denial of Service	oracle-tns	5.0
Oracle Database exp.exe Parameter Remote Buffer Overflow Vulnerability	oracle-tns	5.0
Oracle Spatial Remote Security Bypass	oracle-tns	5.0
Oracle Enterprise Manager Grid Control Privilege Escalation	oracle-tns	5.0
Oracle Database Server Change Data Capture Information Disclosure (CVE-2010-2415)	oracle-tns	5.0
Oracle Database Server Oracle OLAP Remote Authentication Vulnerability (CVE-2010-0902)	oracle-tns	5.0
Oracle Database RDBMS Component Information Disclosure Vulnerability (CVE-2009-3410)	oracle-tns	4.0
Oracle Database Vault SYSDBA Denial of Service	oracle-tns	4.0
Oracle Database Server Core RDBMS Information Disclosure (CVE-2010-2391)	oracle-tns	4.0

Vulnerabilities	Service	Level Risk
Oracle Database Server Export Component Remote Authentication Security Bypass	oracle-tns	4.0
Oracle Database Server Database Vault Denial of Service II	oracle-tns	4.0
Oracle XDK Denial Of Service (CVE-2010-2407)	oracle-tns	4.0
Oracle Database Server Database Vault Denial of Service I	oracle-tns	4.0
Oracle Database Server Network Layer Remote Authentication Bypass Vulnerability (CVE-2010-0900)	oracle-tns	4.0
Oracle Database Logical Standby Component Information Disclosure Vulnerability	oracle-tns	4.0
Oracle Database Audit Component Vulnerability (CVE-2010-0854)	oracle-tns	2.0
Oracle Database Server Perl Information Disclosure (CVE-2010-2389)	oracle-tns	1.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Oracle Database Server Version Information	oracle-tns	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
Oracle Database Obsolete Version Detection	oracle-tns	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-037 - 10.1.171.157

Vulnerabilities	Service	Level Risk
NetBIOS Sessions Using Any Username And Password Are Allowed	microsoft-ds	7.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	microsoft-ds	0.0
Hidden WWW Server Name Detected	http	0.0
Microsoft Windows Anonymous Remote Registry Pipe Access Detected	microsoft-ds	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Windows Anonymous Remote Registry Key Access Detected	microsoft-ds	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-067 - 10.1.171.170

Vulnerabilities	Service	Level Risk
Oracle Database Server TNS Listener Poison Attack Remote Code Execution	oracle-tns	9.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-054 - 10.1.171.176

Vulnerabilities	Service	Level Risk
VNC Server Detected	vnc	0.0
VNC HTTP Console	http	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0

HO-CNTT-TT2-030 - 10.1.171.211

Vulnerabilities	Service	Level Risk
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-029 - 10.1.171.148

Vulnerabilities	Service	Level Risk
IIS IISHelp Default Pages	http	7.0
Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability	http	5.0
Microsoft IIS / RPC Guest Username Disclosure	http	3.0
FTP Anonymous User Account ftp Accessible	ftp	3.0
Microsoft IIS Tilde Character Short File Name Disclosure (142982)	http	3.0
Web Server Default Welcome Page	http	1.0
NetBIOS Bindings Information Detected	netbios-ns	0.0
Microsoft ASP.NET HTTP Handlers Enumeration	http	0.0
Microsoft IIS Localstart Page Authentication Interface Brute Force	http	0.0

Vulnerabilities	Service	Level Risk
VNC Server Detected	vnc	0.0
NetBIOS NBTSTAT -A	netbios-ns	0.0
FTP Server Detected	ftp	0.0
Microsoft ASP.NET State Service Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft IIS Printers Directory Authentication Interface Brute Force	http	0.0
FTP Server With Clear Text Authentication Detected	ftp	0.0
Microsoft Windows IIS ASP.NET Version Detection	http	0.0
Microsoft IIS Server Script Mapping Configuration Presence Detected	http	0.0
SMTP Server Connection Allowed	smtp	0.0
Microsoft Internet Information Services (IIS) Obsolete Version Detection	http	0.0
Microsoft IIS FrontPage Extensions Enabled	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
Web Server HTTP TRACE Method Enabled	http	0.0
FTP Server Found	ftp	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Web Server Default Installation Page Detected	http	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
Microsoft IIS Server Extensions Enumerated	http	0.0
Microsoft IIS Server Detected	http	0.0
Web Server WebDAV Detected	http	0.0
Microsoft IIS Host Name Setting Enumerated	http	0.0
HTTP Server Set Cookies Detected	http	0.0
Microsoft IIS Anonymous Access Enabled	http	0.0
NetBIOS Names Information Accessible	netbios-ns	0.0
SMTP Server Detected	smtp	0.0

Vulnerabilities	Service	Level Risk
Hidden WWW Server Name Detected	http	0.0
Microsoft IIS WebDav Enabled	http	0.0

HO-CNTT-TT2-005 - 10.1.171.141

Vulnerabilities	Service	Level Risk
VNC Server Detected	vnc	0.0
VNC HTTP Console	http	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0

HO-CNTT-TT2-014 - 10.1.171.158

Vulnerabilities	Service	Level Risk
NetBIOS Sessions Using Any Username And Password Are Allowed	microsoft-ds	7.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	microsoft-ds	0.0
Hidden WWW Server Name Detected	http	0.0
Microsoft Windows Anonymous Remote Registry Pipe Access Detected	microsoft-ds	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Windows Anonymous Remote Registry Key Access Detected	microsoft-ds	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-019 - 10.1.171.168

Vulnerabilities	Service	Level Risk
Oracle Database Server TNS Listener Poison Attack Remote Code Execution	oracle-tns	9.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-025 - 10.1.171.174

Vulnerabilities	Service	Level Risk
Oracle Database Server TNS Listener Poison Attack Remote Code Execution	oracle-tns	9.0
VNC Server Detected	vnc	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

HO-CNTT-TT2-044 - 10.1.171.194

Vulnerabilities	Service	Level Risk
Microsoft IIS NTLM Authentication Disabled	http	0.0
VNC Server Detected	vnc	0.0
Microsoft IIS Server Detected	http	0.0
VNC HTTP Console	http	0.0
Microsoft Terminal Service Has Not Been Configured Network Level Authentication	ms-term-service	0.0
Hidden WWW Server Name Detected	http	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0

Vulnerabilities In Detail

Oracle Database Listener Component Information Disclosure Vulnerability

Vulnerbility:		Oracle Database Listener Component Information Disclosure Vulnerability	
Level Risk:		10.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0071

Observation:
A vulnerability exists in the Listener component of Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.7 that could result in the unwanted disclosure of information. The vulnerability is an unspecified vulnerability that could allow a remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2010) available here: http://www.oracle.com/technetwork/topics/security/cpujan2010-084891.html

Description:
A vulnerability exists in the Listener component of Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.7 that could result in the unwanted disclosure of information.

Oracle Database Critical Patch Update April 2013

Vulnerbility:		Oracle Database Critical Patch Update April 2013	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2013-1534

Observation:
Oracle Database is a popular enterprise class database software. Multiple vulnerabilities are present in some versions of Oracle Database. The flaw lies in the Workload Manager, Application Express, and Network Layer component. Successful exploitation could allow an attacker to execute remote code or cause a denial of service (DoS).

Recommendation:
The vendor has released an advisory to address the issues: http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html

Description:
Multiple vulnerabilities are present in some versions of Oracle Database.

Oracle Database Server Oracle Text Privilege Escalation

Vulnerbility:		Oracle Database Server Oracle Text Privilege Escalation	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2011-2301

Observation:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html

Description:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Oracle Database Server January 2013 Critical Patch Update

Vulnerbility:		Oracle Database Server January 2013 Critical Patch Update	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2012-3220

Observation:
Oracle Database is a popular enterprise class database software. Multiple vulnerabilities are present in some versions of Oracle Database. The flaw lies in the Oracle Net protocol of the Spatial component. Successful exploitation could allow an attacker to execute remote code. The exploit requires the attacker to have valid credentials to the vulnerable system.

Recommendation:
The vendor has released an advisory to address the issues. http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html

Description:
Multiple vulnerabilities are present in some versions of Oracle Database.

Oracle Database Server TNS Listener Poison Attack Remote Code Execution

Vulnerbility:		Oracle Database Server TNS Listener Poison Attack Remote Code Execution	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2012-1675

Observation:
A remote code execution vulnerability is present in some versions of Oracle Database Server.The flaw lies in the TNS Listener component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

Description:
A remote code execution vulnerability is present in some versions of Oracle Database Server.

Oracle Database April 2012 Critical Patch Update

Vulnerbility:		Oracle Database April 2012 Critical Patch Update	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2012-0552

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities are present in Oracle Database. Vulnerabilities exist in Oracle Database that may allow for a complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication.

Recommendation:
Download the latest version of Oracle Database from the following location: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html http://metalink.oracle.com/

Description:
Multiple vulnerabilities are present in Oracle Database.

Oracle Database October 2011 Critical Patch Update

Vulnerbility:		Oracle Database October 2011 Critical Patch Update	
Level Risk:		9.0	
Service:	oracle-tns	**CVE:**	CVE-2011-3512

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2011.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for October 2011 to address these. The affected components are:Oracle Database 11g Release 2, version 11.2.0.2 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Oracle Database 10g Release 1, version 10.1.0.5

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - October 2011) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html

Description:
Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2011.

Oracle Database Server Listener Oracle Net Remote Authentication Bypass Vulnerability (CVE-2010-0911)

Vulnerbility:		Oracle Database Server Listener Oracle Net Remote Authentication Bypass Vulnerability (CVE-2010-0911)	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0911

Observation:
A Remote Authentication bypass vulnerability exists in few versions of Oracle Database Server.A vulnerability in the Listener component in Oracle Database Server allows remote attackers to affect availability without the need for a username and password.

Recommendation:
The vendor has addressed this issue by providing updates. http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:
A Remote Authentication bypass vulnerability exists in few versions of Oracle Database Server.

Oracle Database October 2009 Critical Patch Update

Vulnerbility:		Oracle Database October 2009 Critical Patch Update	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2009-1007

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2009.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for October 2009 to address these. The affected components are:Oracle Database 11g, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 Oracle Database 10g, version 10.1.0.5 Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - October 2009) available here: http://metalink.oracle.com/ It is recommended to maintain the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html

Description:
Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2009.

Oracle Database October 2010 Critical Patch Update

Vulnerbility:		Oracle Database October 2010 Critical Patch Update	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2010-1321

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2010.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for October 2010 to address these. The affected components are:Oracle Database 11g Release 2, version 11.2.0.1 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 Oracle Database 10g, Release 1, version 10.1.0.5

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - October 2010) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2010.

Oracle Database April 2010 Critical Patch Update

Vulnerbility:		Oracle Database April 2010 Critical Patch Update	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0851

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for April 2010.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for April 2010 to address these. The affected components are:Oracle Database 11g Release 2, version 11.2.0.1 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 Oracle Database 10g, version 10.1.0.5 Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - April 2010) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for April 2010.

Oracle Database July 2010 Critical Patch Update

Vulnerbility:		Oracle Database July 2010 Critical Patch Update	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0892

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for July 2010.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for July 2010 to address these. The affected components are:? Oracle Database 11 g Release 2, version 11.2.0.1 ? Oracle Database 11 g Release 1, version 11.1.0.7 ? Oracle Database 10 g Release 2, versions 10.2.0.3, 10.2.0.4 ? Oracle Database 10 g, version 10.1.0.5 ? Oracle Database 9 i Release 2, versions 9.2.0.8, 9.2.0.8DV

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - July 2010) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for July 2010.

Oracle Database January 2010 Critical Patch Update

Vulnerbility:		Oracle Database January 2010 Critical Patch Update	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2009-1996

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2010.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for January 2010 to address these. The affected components are:Oracle Database 11g, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 Oracle Database 10g, version 10.1.0.5 Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2010) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpujan2010-084891.html

Description:

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2010.

Oracle Database Core RDBMS Component Vulnerability (CVE-2010-0860)

Vulnerbility:		Oracle Database Core RDBMS Component Vulnerability (CVE-2010-0860)	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0860

Observation:
Oracle database is the world's most popular and widely used DB across enterprises.An unspecified vulnerability exists in the core RDBMS component for some versions of Oracle Database that allows malicious remote network traffic to affect the confidentiality, integrity, and availability of a target system.

Recommendation:
The vendor has released an advisory stating the critical patch updates available: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
An unspecified vulnerability exists in the core RDBMS component for some versions of Oracle Database that allows malicious remote network traffic to affect the confidentiality,integrity, and availability of a target system.

Oracle Database Critical Patch Update July 2013

Vulnerbility:		Oracle Database Critical Patch Update July 2013	
Level Risk:		8.0	
Service:	oracle-tns	**CVE:**	CVE-2013-3751

Observation:
Oracle Database is a popular enterprise class database software. Multiple vulnerabilities are present in some versions of Oracle Database. The flaw lies in the XML Parser, Network Layer, Oracle executable and Core RDBMS component. Successful exploitation could allow an attacker to execute remote code.

Recommendation:
The vendor has released an advisory to address the issues: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html

Description:
Multiple vulnerabilities are present in some versions of Oracle Database.

Oracle Database Server Net Foundation Layer Remote Authentication Bypass Vulnerability (CVE-2010-0903)

Vulnerbility:		Oracle Database Server Net Foundation Layer Remote Authentication Bypass Vulnerability (CVE-2010-0903)	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0903

Observation:

A remote authentication bypass vulnerability exists in some versions of Oracle Database Server.An unspecified vulnerability in the Net Foundation Layer component in Oracle Database Server 9.2.0.8, 10.1.0.5, 10.2.0.4, 11.1.0.7, and 11.2.0.1, when running on Windows, allows remote attackers to affect availability via unknown vectors.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:

A remote authentication bypass vulnerability exists in some versions of Oracle Database Server.

Oracle Database Server Change Data Capture GSS-API Library Denial Of Service (CVE-2010-1321)

Vulnerbility:		Oracle Database Server Change Data Capture GSS-API Library Denial Of Service (CVE-2010-1321)	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2010-1321

Observation:

A denial of service vulnerability is present in some versions of Oracle Database.The vulnerability is present in the Change Data Capture component of Oracle Database. Exploitation can cause remote authenticated users to perform a denial of service (NULL pointer dereference and daemon crash) through the GSS-API library.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:

A denial of service vulnerability is present in some versions of Oracle Database.

Oracle Database July 2011 Critical Patch Update

Vulnerbility:		Oracle Database July 2011 Critical Patch Update	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2011-2239

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for July 2011.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for July 2011 to address these. The affected components are:Oracle Database 11g Release 2, versions 11.2.0.1, 11.2.0.2 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Oracle Database 10g Release 1, version 10.1.0.5

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - July 2011) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html

Description:

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for July 2011.

Oracle Database and Enterprise Manager Grid Control Remote Code Execution

Vulnerbility:		Oracle Database and Enterprise Manager Grid Control Remote Code Execution	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2010-3600

Observation:

A remote code execution vulnerability is present in some versions of Oracle Database.This flaw allows remote attackers to execute arbitrary code on vulnerable installations of Oracle Database 11g. Authentication is not required to exploit this issue. The specific vulnerability exists within JSP script which allows clients to upload XML files to the server, exposed via an HTTPS server running by default on TCP port 1158.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:

A remote code execution vulnerability is present in some versions of Oracle Database.

Oracle Database Server Java SecurityManager Remote Code Execution (CVE-2010-2419)

Vulnerbility:		Oracle Database Server Java SecurityManager Remote Code Execution (CVE-2010-2419)	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2419

Observation:

A race condition vulnerability exists in the SecurityManager implementation of the "Java Virtual Machine" component which can be exploited by authenticated users to execute remote code outside of the sandbox. This vulnerability allows remote attackers to break out of the Java Sandbox implemented by Oracle's relational database. Authentication is required to create a Java stored procedure to trigger the issue. The attacker must have 'Create Session' privileges in order to exploit. Successful exploitation allows the attacker to execute arbitrary code.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:

A race condition vulnerability exists in the SecurityManager implementation of the "Java Virtual Machine" component which can be exploited by authenticated users to execute remote code outside of the sandbox.

Oracle Database Server October 2012 Critical Patch Update

Vulnerbility:		Oracle Database Server October 2012 Critical Patch Update	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2012-3137

Observation:

Oracle Database is a popular enterprise class database software. Multiple vulnerabilities are present in some versions of Oracle Database. The flaws lie in multiple components, Successful exploitation could allow an attacker to execute arbitrary code.

Recommendation:

The vendor has released an advisory to address the issues. http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html

Description:

Multiple vulnerabilities are present in some versions of Oracle Database.

NetBIOS Sessions Using Any Username And Password Are Allowed

Vulnerbility:		NetBIOS Sessions Using Any Username And Password Are Allowed	
Level Risk:		7.0	
Service:	microsoft-ds	**CVE:**	CVE-1999-0519

Observation:
The Network Basic Input/Output System (NetBIOS) is an Application Programming Interface (API) that allows computers to communicate over a network. The host allows remote computers to establish a NetBIOS session using any username and password. On a Microsoft Windows machine, this indicates that the Guest account has a blank password.

Recommendation:
On Windows systems, disable the Guest account or at least set a non-blank password for the account.For Samba on Linux, set the following in the smb.conf file: guest account = NO_SUCH_USER restrict anonymous = yeswhere NO_SUCH_USER is not a valid user in the password file. For other Unix based operating systems, refer the vendor specific documentation and restrict Samba guest account and anonymous login by making necessary changes in the Samba configuration file.

Description:
The host allows remote computers to establish a NetBIOS session using any username and password.

IIS IISHelp Default Pages

Vulnerbility:		IIS IISHelp Default Pages	
Level Risk:		7.0	
Service:	http	**CVE:**	CVE-2002-0074

Observation:
The /IISHelp folder comes with the Microsoft IIS web server and provides additional help documentation for server administrators. Help and example folders that ship with web servers often are found to either contain vulnerabilities (such as cross site scripting attacks) or provide privileged information to an attacker. These default example folders should always be removed.

Recommendation:
Default web folders and their associated contents should be removed.

Description:
The /IISHelp folder was found on the IIS web server.

Oracle Database Server OLAP Information Disclosure (CVE-2010-2412)

Vulnerbility:		Oracle Database Server OLAP Information Disclosure (CVE-2010-2412)	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2412

Observation:

An information disclosure vulnerability is present in some versions of Oracle Database.An unspecified vulnerability is present in the OLAP component of Oracle Database. Exploitation of the vulnerability causes remote authenticated attackers to disclose or manipulate certain information.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:

An information disclosure vulnerability is present in some versions of Oracle Database.

Oracle Database CTXSYS.CONTEXT Privilege Escalation Vulnerability

Vulnerbility:		Oracle Database CTXSYS.CONTEXT Privilege Escalation Vulnerability	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2012-3132

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.A privilege escalation vulnerability is present in some versions of Oracle Database Server. The issue lies in CTXSYS.CONTEXT. Successful exploitation could allow an attacker to get SYSDBA privileges.

Recommendation:

Download the latest version of Oracle Database from the following location: http://www.oracle.com/technetwork/topics/security/alert-cve-2012-3132-1721017.html

Description:

A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Oracle Database July 2012 Critical Patch Update

Vulnerbility:		Oracle Database July 2012 Critical Patch Update	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2012-1737

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities are present in some versions of Oracle Database. Vulnerabilities exist in Oracle Database that may allow for attackers to affect availability.

Recommendation:

Download the latest version of Oracle Database from the following location: http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html http://metalink.oracle.com/

Description:

Multiple vulnerabilities are present in some versions of Oracle Database.

Oracle Database January 2011 Critical Patch Update

Vulnerbility:		Oracle Database January 2011 Critical Patch Update	
Level Risk:		6.0	
Service:	oracle-tns	**CVE:**	CVE-2010-3600

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2011.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for January 2011 to address these. The affected components are:Oracle Database 11g Release 2, version 11.2.0.1 Database Oracle Database 11g Release 1, version 11.1.0.7 DatabaseOracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Database Oracle Database 10g Release 1, version 10.1.0.5

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2011) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2011.

Oracle Database April 2011 Critical Patch Update

Vulnerbility:		Oracle Database April 2011 Critical Patch Update	
Level Risk:		6.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0792

Observation:

Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for April 2011.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for April 2011 to address these. The affected components are:Oracle Database 11g Release 2, versions 11.2.0.1, 11.2.0.2 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Oracle Database 10g Release 1, version 10.1.0.5

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - April 2011) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for April 2011.

Oracle Fusion Middleware Help Security Bypass

Vulnerbility:		Oracle Fusion Middleware Help Security Bypass	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0785

Observation:
A security bypass vulnerability is present in some versions of Oracle Database Server.The flaw lies in the Oracle Help Component. Successful exploitation could allow an attacker to affect integrity via unknown vectors.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A security bypass vulnerability is present in some versions of Oracle Database Server.

Oracle Database Network Foundation Denial of Service

Vulnerbility:		Oracle Database Network Foundation Denial of Service	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0806

Observation:
A denial of service vulnerability is present in some versions of Oracle Database Server.The flaw lies in the Network Foundation component. Successful exploitation could allow an attacker to affect availability via unknown vectors.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A denial of service vulnerability is present in some versions of Oracle Database Server.

Oracle Database Server Job Queue Remote Code Execution (CVE-2010-2411)

Vulnerbility:		Oracle Database Server Job Queue Remote Code Execution (CVE-2010-2411)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2411

Observation:
A remote code execution vulnerability is present in some versions of Oracle Database.The vulnerability is present in the Job Queue component of Oracle Database, related to SYS.DBMS_IJOB. Exploitation of the vulnerability allows remote authenticated users to execute arbitrary code.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
A remote code execution vulnerability is present in some versions of Oracle Database.

Oracle Database exp.exe Parameter Remote Buffer Overflow Vulnerability

Vulnerbility:		Oracle Database exp.exe Parameter Remote Buffer Overflow Vulnerability	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	-

Observation:
Oracle Database is a widely used relational database management system.A buffer overflow vulnerability is present in some versions of Oracle Database server. A flaw is present in the export utility (exp.exe), which fails to validate user supplied data when processing a parameter file (PARFILE). Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

Recommendation:
Download the latest version of Oracle Database from the following location: http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

Description:
A buffer overflow vulnerability is present in some versions of Oracle Database server.

Oracle Database Data Pump Component Vulnerability (CVE-2009-3411)

Vulnerbility:		Oracle Database Data Pump Component Vulnerability (CVE-2009-3411)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2009-3411

Observation:
A vulnerability exists in the Data Pump component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV that could allow for the unwanted disclosure of information and/or a denial of service.

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2010) available here: http://www.oracle.com/technetwork/topics/security/cpujan2010-084891.html

Description:
A vulnerability exists in the Data Pump component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV that could allow for the unwanted disclosure of information and/or a denial of service.

Oracle Enterprise Manager Grid Control Privilege Escalation

Vulnerbility:		Oracle Enterprise Manager Grid Control Privilege Escalation	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0787

Observation:
A privilege escalation vulnerability is present in some versions of Oracle Enterprise Manager Grid Control.The flaw lies in the Application Service Level Management component. Successful exploitation could allow an attacker to affect confidentiality and integrity via unknown vectors.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A privilege escalation vulnerability is present in some versions of Oracle Enterprise Manager Grid Control.

Oracle Database Server Change Data Capture Information Disclosure (CVE-2010-2415)

Vulnerbility:		Oracle Database Server Change Data Capture Information Disclosure (CVE-2010-2415)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2415

Observation:
An information disclosure vulnerability is present in some versions of Oracle Database.The vulnerability is related to the DBMS_CDC_PUBLISH in the Change Data Capture component in Oracle Database Server. Exploitation of this vulnerability allows remote authenticated users to disclose information and manipulate data.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
An information disclosure vulnerability is present in some versions of Oracle Database.

Oracle Database Server Oracle OLAP Remote Authentication Vulnerability (CVE-2010-0902)

Vulnerbility:		Oracle Database Server Oracle OLAP Remote Authentication Vulnerability (CVE-2010-0902)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0902

Observation:
A remote authentication vulnerability exists in some versions of Oracle Database Server Oracle OLAP componentAn unspecified vulnerability in the Oracle OLAP component in Oracle Database Server 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, 11.1.0.7, and 11.2.0.1 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. Because Oracle doesn't provide patches for unsupported version, the unsupported versions are considered as affected.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:
A remote authentication vulnerability exists in some versions of Oracle Database Server Oracle OLAP component.

Oracle Database Server Core RDBMS Privilege Escalation

Vulnerbility:		Oracle Database Server Core RDBMS Privilege Escalation	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-3512

Observation:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html

Description:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability

Vulnerbility:		Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability	
Level Risk:		5.0	
Service:	http	**CVE:**	CVE-2002-1908

Observation:
Microsoft Internet Information Server (IIS) is a popular web server for the Windows platformA denial of service vulnerability is present in some versions of Microsoft IIS. It is possible to reproduce this condition by sending a HTTP POST request with a HOST header field that is composed of an excessive number of slashes (/). Successful exploitation could allow an attacker to cause a denial of service.

Recommendation:
Download the latest version of the Microsoft IIS from the following location: http://www.iis.net/downloads

Description:
A denial of service vulnerability is present in some versions of Microsoft IIS.

Oracle Database Scheduler Agent Information Disclosure

Vulnerbility:		Oracle Database Scheduler Agent Information Disclosure	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-4413

Observation:
An information disclosure vulnerability is present in some versions of Oracle Database Scheduler Agent.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:
An information disclosure vulnerability is present in some versions of Oracle Database Scheduler Agent.

Oracle Database Vault Remote Security Bypass I

Vulnerbility:		Oracle Database Vault Remote Security Bypass I	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-4420

Observation:
A remote security bypass vulnerability is present in some versions of Oracle database vault.The flaw can be exploited over the HTTP protocol and attackers do not require privileges to exploit it.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:
A remote security bypass vulnerability is present in some versions of Oracle database vault.

Oracle Spatial Remote Security Bypass

Vulnerbility:		Oracle Spatial Remote Security Bypass	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-3590

Observation:
A remote security bypass vulnerability is present in some versions of Oracle Spatial.The flaw can be exploited over the Oracle Net protocol and an attacker with execute on MDSYS procedures privilege can exploit it.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:
A remote security bypass vulnerability is present in some versions of Oracle Spatial.

Oracle Database Server Listener Oracle Net Denial Of Service

Vulnerbility:		Oracle Database Server Listener Oracle Net Denial Of Service	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2012-0072

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.A denial of service vulnerability in Core RDBMS is present in some versions of Oracle Database Server.The flaw lies in listener component of the Core RDBMS. Attackers can exploit this issue to cause partial denial of service conditions.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Description:
A denial of service vulnerability in Core RDBMS is present in some versions of Oracle Database Server.

Oracle Database JavaVM Component Vulnerability (CVE-2010-0867)

Vulnerbility:		Oracle Database JavaVM Component Vulnerability (CVE-2010-0867)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0867

Observation:
Oracle database is a popular and widely used database across enterprises. An unspecified vulnerability exists in the JavaVM component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Recommendation:
The vendor has released an advisory stating the critical patch updates available: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
An unspecified vulnerability exists in the JavaVM component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Oracle Database Vault Privilege Escalation

Vulnerbility:		Oracle Database Vault Privilege Escalation	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0804

Observation:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.The flaw lies in the Database Vault component. Successful exploitation could allow an attacker to affect confidentiality and integrity.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A privilege escalation vulnerability is present in some versions of Oracle Database Server.

Oracle Database Vault Remote Security Bypass

Vulnerbility:		Oracle Database Vault Remote Security Bypass	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-4421

Observation:
A remote security bypass vulnerability is present in some versions of Oracle database vault. The flaw can be exploited over the HTTP protocol and attackers do not require privileges to exploit it.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:
A remote security bypass vulnerability is present in some versions of Oracle database vault.

Oracle Database Server Core RDBMS Create Session Information Disclosure

Vulnerbility:		Oracle Database Server Core RDBMS Create Session Information Disclosure	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2012-0082

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle. An information disclosure vulnerability in Core RDBMS is present in some versions of Oracle Database Server.The flaw can be exploited in the core RDBMS to partially modify data on the target system . The attacker must have 'Create session' privileges for a successful exploitation.

Recommendation:
Download the latest version of Oracle Core RDBMS from the following location : http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Description:
An information disclosure vulnerability in Core RDBMS is present in some versions of Oracle Database Server.

Oracle Database JavaVM Component Vulnerability (CVE-2010-0866)

Vulnerbility:		Oracle Database JavaVM Component Vulnerability (CVE-2010-0866)	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0866

Observation:
Oracle database is the world's most popular and widely used DB across enterprises.An unspecified vulnerability exists in the JavaVM component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Recommendation:
The vendor has released an advisory stating the critical patch updates available: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
An unspecified vulnerability exists in the JavaVM component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Oracle Database January 2012 Critical Patch Update

Vulnerbility:		Oracle Database January 2012 Critical Patch Update	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2012-0082

Observation:
Oracle Database is a popular enterprise class database software developed by Oracle.Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2012.Vulnerabilities exist in Oracle Database that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for January 2012 to address these. The affected components are:Oracle Database 11g Release 2, versions 11.2.0.2, 11.2.0.3 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Oracle Database 10g Release 1, version 10.1.0.5

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2012) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latest releases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Description:
Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for January 2012.

Oracle Database Cluster Verify Utility Privilege Escalation

Vulnerbility:		Oracle Database Cluster Verify Utility Privilege Escalation	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-4423

Observation:
A local privilege escalation vulnerability is present in some versions of Oracle Cluster Verify Utility.The flaw can be exploited over the local protocol and an attacker does not require privileges to exploit it.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

Description:
A local privilege escalation vulnerability is present in some versions of Oracle Cluster Verify Utility.

Oracle Database UIX Security Bypass

Vulnerbility:		Oracle Database UIX Security Bypass	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0805

Observation:
A security bypass vulnerability is present in some versions of Oracle Database Server.The flaw lies in the UIX component. Successful exploitation could allow an attacker to affect integrity via unknown vectors.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A security bypass vulnerability is present in some versions of Oracle Database Server.

Oracle Database DBMS_JAVA.SET_OUTPUT_TO_JAVA Privilege Escalation Vulnerability

Vulnerbility:		Oracle Database DBMS_JAVA.SET_OUTPUT_TO_JAVA Privilege Escalation Vulnerability	
Level Risk:		5.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0866

Observation:
Oracle Database is a widely used relational database management system. A privilege escalation vulnerability is present in some versions of Oracle Database servers. The flaws are present in the server, which fails to restrict access to certain Java set packages. Successful exploitation could allow an attacker to escalate privileges to DBA or SYSTEM.

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Patch Update - April 2010) available here: http://metalink.oracle.com/ It is recommended to keep the Oracle application current with the latestreleases. Specific patch information is available here: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
A privilege escalation vulnerability is present in some versions of Oracle Database servers.

Oracle Database Server Database Vault Denial of Service I

Vulnerbility:		Oracle Database Server Database Vault Denial of Service I	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2011-3511

Observation:
A denial of service vulnerability is present in some versions of Oracle Database Server.The flaw is specific to the Database Vault component. Successful exploitation could allow an attacker to cause a denial of service condition.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html

Description:
A denial of service vulnerability is present in some versions of Oracle Database Server.

Oracle Database Server Network Layer Remote Authentication Bypass Vulnerability (CVE-2010-0900)

Vulnerbility:		Oracle Database Server Network Layer Remote Authentication Bypass Vulnerability (CVE-2010-0900)	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0900

Observation:
A remote authentication bypass vulnerability exists in few versions of Oracle Database Server.This issue in the Network Layer component in Oracle Database Server allows remote attackers to affect availability without the need for a user name and password.

Recommendation:
The vendor has addressed this issue by providing updates. http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:
A remote authentication bypass vulnerability exists in few versions of Oracle Database Server.

Oracle Database RDBMS Component Information Disclosure Vulnerability (CVE-2009-3410)

Vulnerbility:		Oracle Database RDBMS Component Information Disclosure Vulnerability (CVE-2009-3410)	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2009-3410

Observation:
A vulnerability exists in the RDBMS component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV that could result in the unwanted disclosure of information.

Recommendation:
The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2010) available here: http://www.oracle.com/technetwork/topics/security/cpujan2010-084891.html

Description:
A vulnerability exists in the RDBMS component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV that could result in the unwanted disclosure of information.

Oracle Database Server Core RDBMS Information Disclosure (CVE-2010-2391)

Vulnerbility:		Oracle Database Server Core RDBMS Information Disclosure (CVE-2010-2391)	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2391

Observation:
An information disclosure vulnerability is present in some versions of the Oracle Database.This vulnerability in the Core RDBMS component in Oracle Database Server allows remote authenticated users to affect confidentiality and integrity via unknown vectors.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
An information disclosure vulnerability is present in some versions of the Oracle Database.

Oracle Database Vault SYSDBA Denial of Service

Vulnerbility:		Oracle Database Vault SYSDBA Denial of Service	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2011-0793

Observation:
A denial of service vulnerability is present in some versions of Oracle Database Server.The flaw lies in the Database Vault component of the SYSDBA package. Successful exploitation could allow an attacker to affect integrity and availability.

Recommendation:
The vendor has released an update to address the issue: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Description:
A denial of service vulnerability is present in some versions of Oracle Database Server.

Oracle XDK Denial Of Service (CVE-2010-2407)

Vulnerbility:		Oracle XDK Denial Of Service (CVE-2010-2407)	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2407

Observation:
A denial of service vulnerability is present in some versions of Oracle Database.An unspecified vulnerability is present in Oracle Database. This can be exploited by malicious, local users to manipulate certain data.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
A denial of service vulnerability is present in some versions of Oracle Database.

Oracle Database Server Export Component Remote Authentication Security Bypass

Vulnerbility:		Oracle Database Server Export Component Remote Authentication Security Bypass	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0901

Observation:
A remote authentication vulnerability exists in versions of Oracle's Database Server.A vulnerability in the Export component in Oracle Database Server allows remote attackers to affect confidentiality.

Recommendation:
The vendor has addressed this issue by providing udpates. http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html

Description:
A remote authentication vulnerability exists in versions of Oracle's Database Server.

Oracle Database Logical Standby Component Information Disclosure Vulnerability

Vulnerbility:		Oracle Database Logical Standby Component Information Disclosure Vulnerability	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2009-1996

Observation:

Oracle Database Server is an industry-standard database solution.A vulnerability exists in the Logical Standby component in Oracle Database that could allow an unauthorized user to gain elevated privileges.

Recommendation:

The vendor has released patches for remediation to registered users (Oracle Critical Update - January 2010) available here: http://www.oracle.com/technetwork/topics/security/cpujan2010-084891.html

Description:

A vulnerability exists in the Logical Standby component in Oracle Database that could allow an unauthorized user to gain elevated privileges.

Oracle Database Server Database Vault Denial of Service II

Vulnerbility:		Oracle Database Server Database Vault Denial of Service II	
Level Risk:		4.0	
Service:	oracle-tns	**CVE:**	CVE-2011-2322

Observation:

A denial of service vulnerability is present in some versions of Oracle Database Server.The flaw is specific to the Database Vault component. Successful exploitation could allow an attacker to cause a denial of service condition.

Recommendation:

The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html

Description:

A denial of service vulnerability is present in some versions of Oracle Database Server.

FTP Anonymous User Account ftp Accessible

Vulnerbility:		FTP Anonymous User Account ftp Accessible	
Level Risk:		3.0	
Service:	ftp	**CVE:**	CVE-1999-0497

Observation:

Many default installations of the FTP service allow attackers to login to the FTP server with an anonymous a username of 'ftp' and password consisting of an email address. This capability allows attackers to enumerate a system and increases the risk that a full compromise will occur. Vulnerable Systems: All systems with Anonymous FTP

Recommendation:

Create accounts for specific users that need access to FTP, and enforce a strong password policy. Restrict access to resources on the FTP server that are necessary to perform the needed tasks for each specific user.Disable anonymous ftp if it is not necessary to the system. Restrict read/write permissions if the functionality is needed and restrict the directory that anonymous ftp accesses. Disable ftp if it is not necessary by commenting it out of the etc/inetd.conf file. #ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a Restart the inet process #kill -HUP (pid of inetd) UNIX ----Add users to the /etc/ftpusers file who should not be allowed access to the system via FTP; examples are root, bin, guest, shutdown, lp, user1, user2, user3 To enable Anonymous FTP more securely:1. Create the correct home directories for exclusive use of ftpd, such as ~ftp/bin, ~ftp/etc, and ~ftp/pub. 2. Create an FTP account that points to the FTP home directory3. Change the FTP passwd file to contain entries only for root and FTP.4. Change the group file to contain only the FTP group.5. Change permissions on files and directories to appropriate users. Windows ------- By default, the Windows FTP service allows for anonymous connections. To turn off this feature follow these steps: 1. Start the Internet Service Manager2. Select the FTP site running and click on Properties3. Select the Security Accounts tab 4. Uncheck the 'Allow Anonymous Connections' box. When prompted, click Yes to continue.

Description:

A vulnerability in the configuration of FTP servers allows remote attackers to connect with user 'ftp' and an email address for the password.

Microsoft IIS Tilde Character Short File Name Disclosure (142982)

Vulnerbility:		Microsoft IIS Tilde Character Short File Name Disclosure (142982)	
Level Risk:		3.0	
Service:	http	**CVE:**	-

Observation:

IIS is a web server application and a set of feature extension modules created by Microsoft.There is an information disclosure vulnerability present in some versions of Microsoft IIS. This flaw can be exploited by sending a GET request with a tilde character "~" in the request, it could allow remote attackers to disclose files and folders names based on return status code. The same vulnerability could also cause a denial of service condition.

Recommendation:

McAfee is currently unaware of a vendor-supplied patch or update (2016-11-10) The vendor has released an advisory describing a workaround that can be used to mitigate this issue. More information can be found at: http://support.microsoft.com/kb/121007 http://support.microsoft.com/kb/142982/en-us

Description:

There is an information disclosure vulnerability present in some versions of Microsoft IIS.

Microsoft IIS / RPC Guest Username Disclosure

Vulnerbility:		Microsoft IIS / RPC Guest Username Disclosure	
Level Risk:		3.0	
Service:	http	**CVE:**	CVE-2000-0114

Observation:
Microsoft Internet Information Server (IIS) is an industry standard HTTP serverMicrosoft Frontpage Extensions support RPC functionality via HTTP.By performing an RPC request that is designed to fail due to security restrictions it is possible to generate an error message that contains the username of the account denied access to the requested resource. Vulnerable Systems: Microsoft IIS 4.0, 5.0

Recommendation:
McAfee is currently unaware of a vendor-supplied patch or update (2016-11-18) Please contact the vendor for recommendations: http://www.microsoft.com The following workaround is available: All service pack levels of Microsoft IIS 4.0 and 5.0 are vulnerable. In addition, Microsoft has not released a patch or modified the behavior of IIS to prevent the disclosure of the web guest account username. It is suggested that anonymous access be denied to the /_vti_bin virtual directory. 1. In the IIS configuration program (MMC control panel for IIS 4.0 or Computer Management control panel for IIS 5.0) select the target system\'s default web site. 2. Right-click the /_vti_bin virtual directory for the default web site and select Properties. 3. Select the Directory Security tab from the /_vti_bin Properties window.4. Click the Edit... button in the Anonymous access and authentication control pane of the /_vti_bin Properties window. 5. De-select Anonymous access in the Authentication Methods window. 6. Select OK to close the Authentication Methods window. 7. Select Apply to apply the changes.

Description:
An information disclosure vulnerability exists within Microsoft IIS 4.0 that allows for an attacker to obtain the username of the guest web user account (IUSR_computername).

Oracle Database Audit Component Vulnerability (CVE-2010-0854)

Vulnerbility:		Oracle Database Audit Component Vulnerability (CVE-2010-0854)	
Level Risk:		2.0	
Service:	oracle-tns	**CVE:**	CVE-2010-0854

Observation:
Oracle database is a popular and widely used database across enterprises. An unspecified vulnerability exists in the audit component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Recommendation:
The vendor has released an advisory stating the critical patch updates available: http://www.oracle.com/technetwork/topics/security/cpuapr2010-099504.html

Description:
An unspecified vulnerability exists in the audit component for some versions of Oracle Database that allows malicious remote network traffic to affect the integrity of a target system.

Oracle Database Server Perl Information Disclosure (CVE-2010-2389)

Vulnerbility:		Oracle Database Server Perl Information Disclosure (CVE-2010-2389)	
Level Risk:		1.0	
Service:	oracle-tns	**CVE:**	CVE-2010-2389

Observation:
An Information Disclosure vulnerability is present in some versions of the Oracle Database.This vulnerability in the Perl component in Oracle Database Server allows local users to affect integrity via unknown vectors related to Local Logon.

Recommendation:
The vendor has released an update to address this issue: http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html

Description:
An Information Disclosure vulnerability is present in some versions of the Oracle Database.

Web Server Default Welcome Page

Vulnerbility:		Web Server Default Welcome Page	
Level Risk:		1.0	
Service:	http	**CVE:**	CVE-MAP-NOMATCH

Observation:
The testing, temporary, or default web server welcome page files were found on the server. These temporary files, especially ones that demonstrate scripting capabilities, often have security vulnerabilities present in them and are exploited by attackers.

Recommendation:
If the web server is not in use, the server should be disabled. However, if the server will soon be used, the default welcome and test pages should be removed immediately.

Description:
The web server was found to have its' default welcome page set.

Microsoft IIS Host Name Setting Enumerated

Vulnerbility:		Microsoft IIS Host Name Setting Enumerated	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS "Use Host Header Name" setting is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enable "Use Host Header Name" setting.

Description:
Microsoft Internet Information Services (IIS) "Use Host Header Name" setting is disabled on the host.

Microsoft IIS Server Script Mapping Configuration Presence Detected

Vulnerbility:		Microsoft IIS Server Script Mapping Configuration Presence Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS script mapping configuration was detected on the host.

Recommendation:

Ensure that Microsoft IIS complies with organizational policy.

Description:

Microsoft Internet Information Services (IIS) script mapping configuration was detected on the host.

Microsoft IIS Basic Authentication Scheme Disabled

Vulnerbility:		Microsoft IIS Basic Authentication Scheme Disabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS Basic Authentication scheme is disabled on the host.

Recommendation:

Ensure that Microsoft IIS complies with the corporate policy.

Description:

Microsoft Internet Information Services (IIS) Basic Authentication scheme is disabled on the host.

VNC HTTP Console

Vulnerbility:		VNC HTTP Console	
Level Risk:		0.0	
Service:	http	**CVE:**	CVE-MAP-NOMATCH

Observation:

The Virtual Network Computing (VNC) software package allows for a user to remotely access a graphical desktop environment. The VNC package includes functionality that allows for a user to gain remote console access by connecting a Java enabled web browser to a VNC HTTP serverPerforming an HTTP GET for the root directory returned one or more files that are part of the VNC HTTP remote console package. For more information see: VNC http://www.uk.research.att.com/vnc/

Recommendation:

If VNC is not required on the server, it is highly recommended to remove all of its files.To do so, follow the instructions below: Removing VNC ----- For Microsoft Windows:1. Go to start, settings, and then control panel. 2. Then click on Add/Remove programs. 3. In there, you should see VNC Server. 4. Uninstall VNC Server.

Description:

A VNC HTTP remote desktop console was detected.

Microsoft Windows Terminal Service

Vulnerbility:		Microsoft Windows Terminal Service	
Level Risk:		0.0	
Service:	ms-term-service	**CVE:**	CVE-MAP-NOMATCH

Observation:

Terminal Services allows the remote, full-access administration of any server running Microsoft Windows. This service is optional, and can be disabled at any time. If an attacker gains a valid username and password, he can use this service to gain further access on the remote host. Windows XP uses Terminal Services to provide additional functionality such as Fast User Switch, and Remote Assistance. Vulnerable Systems: Microsoft Windows 2000, NT, XP, 2003

Recommendation:

Disable Terminal Services if not in use. Ensure that account policies for Terminal Server users is as restrictive as possible. To disable Terminal Services: For Windows 2000 and NT1. Click Start > Settings > Control Panel. 2. Double click Add/Remove programs. 3. In the Add/Remove programs window, click Add/Remove Windows Components. 4. Scroll down and click Terminal Services. Then click Next twice to remove it.

Description:

Microsoft Windows Terminal service has been detected on the target host.

Microsoft Internet Information Services (IIS) Obsolete Version Detection

Vulnerbility:		Microsoft Internet Information Services (IIS) Obsolete Version Detection	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformAn obsolete version of Microsoft Internet Information Services (IIS) is detected on the target. The vendor no longer provides support or patches for obsolete versions of the product. Use of vulnerable obsolete software may expose the target system to malicious attacks.

Recommendation:

Upgrade to the latest version of Microsoft Internet Information Services (IIS). http://www.microsoft.com/web/platform/server.aspx

Description:

An obsolete version of Microsoft Internet Information Services (IIS) is detected on the target.

Microsoft IIS Anonymous Access Enabled

Vulnerbility:		Microsoft IIS Anonymous Access Enabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS anonymous access is enabled.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy.

Description:
Microsoft Internet Information Services (IIS) anonymous access is enabled.

Microsoft IIS FrontPage Extensions Enabled

Vulnerbility:		Microsoft IIS FrontPage Extensions Enabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS FrontPage Server Extensions are enabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy.

Description:
Microsoft Internet Information Services (IIS) FrontPage Server Extensions are enabled on the host.

Microsoft IIS NTLM Authentication Disabled

Vulnerbility:		Microsoft IIS NTLM Authentication Disabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS NTLM Authentication is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enforce NTLM authentication for Microsoft IIS.

Description:
Microsoft Internet Information Services (IIS) NTLM Authentication is disabled on the host.

Web Server HTTP TRACE Method Enabled

Vulnerbility:		Web Server HTTP TRACE Method Enabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Web servers are widely used to serve static and dynamic content and render it in the client's browser. HTTP TRACE method is enabled on the HTTP server. This method could be potentially exploited by attacker to obtain sensitive information.

Recommendation:
HTTP TRACE should be disabled on the HTTP server if it is not required.

Description:
HTTP TRACE method is enabled on the HTTP server.

VNC Server Detected

Vulnerbility:		VNC Server Detected	
Level Risk:		0.0	
Service:	vnc	**CVE:**	CVE-MAP-NOMATCH

Observation:
An open VNC connection will allow an attacker to obtain sensitive information about the host and possibly gain access to the system.

Recommendation:
A VNC Server application was detected. The affected system should be examined to determine which VNC application is installed. Once determined, it should be removed unless being used for legitimate business purposes. To uninstall VNC for Windows NT/2000/XP: ----- To uninstall using the Add/Remove Programs control panel: 1. Go to the Start menu, select Settings and then Control Panel. 2. Double-click the Add/Remove Programs icon. 3. Select VNC. 4. Click the Add/Remove button.

Description:
A VNC server has been detected on the host.

SMTP Server Connection Allowed

Vulnerbility:		SMTP Server Connection Allowed	
Level Risk:		0.0	
Service:	smtp	**CVE:**	-

Observation:
SMTP server receives outgoing mail messages from users and forwards to the mail recipients.SMTP server connection was allowed on the host.

Recommendation:
Ensure that SMTP server complies with organizational policy.

Description:
SMTP server connection was allowed on the host.

Web Server Default Installation Page Detected

Vulnerbility:		Web Server Default Installation Page Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Web Server is used to host pages and deliver contents using http protocol. Default installation page was detected on the web server.

Recommendation:
Ensure that the web server complies with organizational policy.

Description:
Default installation page was detected on the web server.

Microsoft ASP.NET HTTP Handlers Enumeration

Vulnerbility:		Microsoft ASP.NET HTTP Handlers Enumeration	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft .NET is a Software Framework for applications designed to run under Microsoft Windows. HTTP handlers in ASP .NET are used for processing different kinds of file types(file extensions). A list of file extensions handled by the ASP.NET server was obtained.

Recommendation:
Ensure that the list of file extension handlers found on the ASP.NET server is allowed by policy.

Description:
A list of file extensions handled by the ASP.NET server was obtained.

Microsoft IIS Server Detected

Vulnerbility:		Microsoft IIS Server Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS was detected on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: Conceal the IIS Server status by modifying the banner.

Description:
Microsoft Internet Information Services (IIS) was detected on the host.

Oracle Database Obsolete Version Detection

Vulnerbility:		Oracle Database Obsolete Version Detection	
Level Risk:		0.0	
Service:	oracle-tns	**CVE:**	-

Observation:

Oracle Database is a popular relational database. An obsolete version of Oracle Database is detected on the target. The vendor no longer provides support or patches for obsolete versions of the product. Use of vulnerable obsolete software may expose the target system to malicious attacks.

Recommendation:

Upgrade to the latest version of Oracle Database.http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

Description:

An obsolete version of Oracle Database is detected on the target.

FTP Server Found

Vulnerbility:		FTP Server Found	
Level Risk:		0.0	
Service:	ftp	**CVE:**	-

Observation:

The File Transfer Protocol (FTP) is a protocol used for transferring files over an Internet Protocol (IP) network. An FTP server was detected on the host.

Recommendation:

Verify that the FTP server's configuration complies with corporate policy.

Description:

An FTP server was detected on the host.

NetBIOS Names Information Accessible

Vulnerbility:		NetBIOS Names Information Accessible	
Level Risk:		0.0	
Service:	netbios-ns	**CVE:**	-

Observation:

Microsoft NetBIOS is a service developed to communicate with different computers over a local network.Microsoft NetBIOS names information was detected on the host.

Recommendation:

Ensure that Microsoft NetBIOS complies with organizational policies.

Description:

Microsoft NetBIOS names information was detected on the host.

Web Server WebDAV Detected

Vulnerbility:		Web Server WebDAV Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. WebDAV was detected on the host.

Recommendation:
Ensure that WebDAV complies with organizational policy.

Description:
WebDAV was detected on the host.

Microsoft ASP.NET State Service Detected

Vulnerbility:		Microsoft ASP.NET State Service Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
The Microsoft ASP.NET State Service is used to manage session state on computerMicrosoft ASP.NET State Service was detected on the host.

Recommendation:
Ensure that Microsoft ASP.NET State service complies with corporate policy.

Description:
Microsoft ASP.NET State Service was detected on the host.

Microsoft Remote Procedure Call Service Detected

Vulnerbility:		Microsoft Remote Procedure Call Service Detected	
Level Risk:		0.0	
Service:	loc-srv	**CVE:**	-

Observation:
Microsoft Remote Procedure Call Service (MSRPC) service is the DCE RPC mechanism implemented by Microsoft. It supports inheritance of interfaces, Unicode strings and implicit handles. Microsoft Remote Procedure Call Service was detected on the host.

Recommendation:
Ensure that MSRPC complies with organizational policy.

Description:
Microsoft Remote Procedure Call Service was detected on the host.

Microsoft Windows IIS ASP.NET Version Detection

Vulnerbility:		Microsoft Windows IIS ASP.NET Version Detection	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft IIS ASP.NET is a software service for applications designed to run under Microsoft Windows. The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

Recommendation:
Ensure that the ASP.NET service is allowed to be running on the host.

Description:
The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

Microsoft Terminal Service Has Not Been Configured Network Level Authentication

Vulnerbility:		Microsoft Terminal Service Has Not Been Configured Network Level Authentication	
Level Risk:		0.0	
Service:	ms-term-service	**CVE:**	-

Observation:
The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication. Network Level Authentication provides better security than previous authentication approach.

Recommendation:
Consider to configure the Terminal Service to use Network Level Authentication if possible.More details could be found at: http://technet.microsoft.com/en-us/library/cc732713.aspx

Description:
The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication.

NetBIOS Bindings Information Detected

Vulnerbility:		NetBIOS Bindings Information Detected	
Level Risk:		0.0	
Service:	netbios-ns	**CVE:**	-

Observation:
NetBIOS is a service which allows different computers to communicate with each other over a local area network.NetBIOS bindings information was detected on the host.

Recommendation:
Ensure that NetBIOS service complies with organizational policies.

Description:
NetBIOS bindings information was detected on the host.

HTTP Server Set Cookies Detected

Vulnerbility:		HTTP Server Set Cookies Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
HTTP servers are widely used to serve static and dynamic content and render it in the client's browser. HTTP cookies are the small piece of state information set on the client application's system, that is used for session handling between web server and client. HTTP server handling session using set-cookie was detected on the host.

Recommendation:
Ensure that HTTP server complies with organizational policy.

Description:
HTTP server handling session using set-cookie was detected on the host.

Microsoft Windows NETBIOS Anonymous Accessible Shares Detected

Vulnerbility:		Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
Microsoft Windows is an industry standard operating system. SMB shares can be accessed anonymously on the Windows host.

Recommendation:
Ensure that Microsoft Windows complies with organizational policy.

Description:
SMB shares can be accessed anonymously on the Windows host.

Oracle Database Server Version Information

Vulnerbility:		Oracle Database Server Version Information	
Level Risk:		0.0	
Service:	oracle-tns	**CVE:**	-

Observation:
Oracle is an enterprise class database application. Oracle has been detected on the target host, and the version information obtained.

Recommendation:
Ensure that the Oracle configuration complies with your corporate policy.

Description:
Oracle has been detected on the target host, and the version information obtained.

Hidden WWW Server Name Detected

Vulnerbility:		Hidden WWW Server Name Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
WWW server is a computer application for delivering web based contents using HTTPHidden WWW server name detected. Web server name can be hidden as a security measure.

Recommendation:
Ensure that web server complies with corporate policy.

Description:
Hidden WWW server name detected.

SMTP Server Detected

Vulnerbility:		SMTP Server Detected	
Level Risk:		0.0	
Service:	smtp	**CVE:**	-

Observation:
SMTP is a standard protocol used for electronic mail transmission across the Internet. SMTP service was detected on the host.

Recommendation:
Ensure that SMTP service complies with organizational policy.

Description:
SMTP service was detected on the host.

Web Server HTTP Protocol Version Detected

Vulnerbility:		Web Server HTTP Protocol Version Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Web servers are widely used to serve static and dynamic content and render it in the client's browser. HTTP protocol version was obtained from the host through web server.

Recommendation:
Ensure that web server complies with organizational policy.

Description:
HTTP protocol version was obtained from the host through web server.

Microsoft IIS WebDav Enabled

Vulnerbility:		Microsoft IIS WebDav Enabled	
Level Risk:		0.0	
Service:	http	**CVE:**	CVE-MAP-NOMATCH

Observation:
Microsoft Internet Information Server (IIS) is an industry standard Web server for the Windows platformInstalled with Windows 2000, IIS 5.0 supports Web-based Distributed Authoring and Versioning (WebDAV) HTTP 1.1 extensions. WebDAV as described in RFC 2518 is used for collaborative remote authoring and versioning of Web content.Vulnerabilities have been discovered in the implementation of WebDAV on IIS. The results of exploitation include denial-of-service and remote command execution on the targeted host. Note: This check is non-intrusive, and looks for the presence of WebDAV on the targeted host. A positive result does not necessarily mean that the host is vulnerable to exploitation through WebDAV. Vulnerable systems: Microsoft Windows 2000 Internet Information Server 5For more information see: Microsoft Security BulletinsMS03-007: http://www.microsoft.com/technet/security/bulletin/MS03-007.mspxMS02-062: http://www.microsoft.com/technet/security/bulletin/MS02-062.mspx

Recommendation:
Disable WebDAV functionality on any server in a production environment. If WebDAV support is necessary, ensure that the latest available patches for are installed on the server. Information on how to obtain and install the patches is available from Microsoft: http://www.microsoft.com/windows2000/downloads/security Microsoft has released the IIS Lockdown tool to enable the security administration of IIS Web servers. The tool includes the ability to block WebDAV functions, and is available from Microsoft: http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC

Description:
WebDAV functionality is enabled on the host.

FTP Server Detected

Vulnerbility:		FTP Server Detected	
Level Risk:		0.0	
Service:	ftp	**CVE:**	-

Observation:
A FTP server is used for transferring files to and from remote systems connected in a network. A FTP server was detected on the host.

Recommendation:
Ensure that the FTP server complies with organizational policy.

Description:
A FTP server was detected on the host.

Microsoft Windows Anonymous Remote Registry Pipe Access Detected

Vulnerbility:		Microsoft Windows Anonymous Remote Registry Pipe Access Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:

Microsoft Windows is an industry standard operating system.Anonymous remote registry access was detected on the Windows host.

Recommendation:

Ensure that Microsoft Windows host complies with organizational policy.

Description:

Anonymous remote registry access was detected on the Windows host.

FTP Server With Clear Text Authentication Detected

Vulnerbility:		FTP Server With Clear Text Authentication Detected	
Level Risk:		0.0	
Service:	ftp	**CVE:**	-

Observation:

A FTP server is used for transferring files to and from remote systems connected in a network.FTP server with clear text authentication was detected on the host.

Recommendation:

Ensure that the FTP server complies with organizational policy.

Description:

FTP server with clear text authentication was detected on the host.

Microsoft IIS Localstart Page Authentication Interface Brute Force

Vulnerbility:		Microsoft IIS Localstart Page Authentication Interface Brute Force	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:

Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformPossibility of brute force authentication against Localstart in Microsoft IIS was detected on the host.

Recommendation:

Ensure that Microsoft IIS complies with organizational policy.

Description:

Possibility of brute force authentication against Localstart in Microsoft Internet Information Services (IIS) was detected on the host.

Web Server Broken Links Detected

Vulnerbility:		Web Server Broken Links Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Web Server is used serve web pages. Web server with broken links was detected on the host.

Recommendation:
Ensure that web server complies with organizational policy.

Description:
Web server with broken links was detected on the host.

NetBIOS NBTSTAT -A

Vulnerbility:		NetBIOS NBTSTAT -A	
Level Risk:		0.0	
Service:	netbios-ns	**CVE:**	CVE-MAP-NOMATCH

Observation:
All Microsoft Windows platforms include support for the NetBIOS network protocol stack. The NetBIOS protocol provides the underlying support for Microsoft Windows file and resource sharing. One component of all Microsoft Windows NetBIOS implementations is the NetBIOS Name Service.The NetBIOS Name Service listens for name service requests on UDP port 137. It can be queried to retrieve a listing of currently logged in user accounts and groups. In addition, the MAC address for the network interface over which the query is performed is included in the response to a nbtstat -A request. The DOS nbtstat command can be used to perform this operation. To do so, open a DOS command prompt and run the following command: nbtstat -A target_system Where target_system is the IP address or hostname of the target system.

Recommendation:
Disable the NetBIOS Name Service to prevent access to NBTSTAT -A informationWorkaround: Block access to UDP port 137 using a firewall. Contact the operating system vendor for hardening steps specific to the operating system.

Description:
It is possible to retrieve NetBIOS Name Service information.

Microsoft Windows Anonymous Remote Registry Key Access Detected

Vulnerbility:		Microsoft Windows Anonymous Remote Registry Key Access Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
Microsoft Windows is an industry standard operating system. Anonymous remote registry key access was detected on the Windows host.

Recommendation:
Ensure that Microsoft Windows host complies with organizational policy.

Description:
Anonymous remote registry key access was detected on the Windows host.

NetBIOS Null Session Enabled

Vulnerbility:		NetBIOS Null Session Enabled	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
A NetBIOS null session allows users to connect to a host remotely with no username and password and perform a limited set of administrative tasks. Null sessions allow the remote user to gather information such as: 1. List users 2. List groups 3. List shares (including hidden shares) 4. Policies (such as minimum password length, etc.) While the enumerated information is not an immediate risk, much of the information can be leveraged to launch an attack to gain user or administrative privilege. All steps should be taken to eliminate the vulnerability and/or reduce the information available to the attacker. This check only attempts to establish a NetBIOS null session with the host. It does not attempt to determine what information is accessible with the null session.

Recommendation:
Disable or restrict null session access to network shares. For Windows operating systems, the configuration steps may vary based on the type of operating system and Domain or Local Security policies. Contact the operating system vendor for hardening steps specific to the operating system and setup environment. For Unix Samba based server, make sure that samba's configuration parameter "guest ok" is set to "no" and set the "restrict anonymous" parameter. Workaround: Block access to TCP port 139 (NetBIOS) and TCP port 445 using a firewallNote: Blocking access for MVM to both TCP ports 139 and 445 will also block MVM's credential based scans. This should only be done if credential based scans are not needed.

Description:
NetBIOS Null sessions are enabled on the host.

Microsoft IIS Server Extensions Enumerated

Vulnerbility:		Microsoft IIS Server Extensions Enumerated	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS server extensions were enumerated on the host.

Recommendation:
Ensure that Microsoft IIS complies with organizational policy.

Description:
Microsoft Internet Information Services (IIS) extensions were enumerated on the host.

Microsoft IIS Printers Directory Authentication Interface Brute Force

Vulnerbility:		Microsoft IIS Printers Directory Authentication Interface Brute Force	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformPossibility of brute force authentication against Printers virtual directory in Microsoft IIS was detected on the host.

Recommendation:
Ensure that Microsoft IIS complies with organizational policy.Note: After backing up the Printers virtual directory, it is advised to rename/remove this directory.

Description:
Possibility of brute force authentication against Printers virtual directory in Microsoft Internet Information Services (IIS) was detected on the host.

LSASS RPC Interface Detected

Vulnerbility:		LSASS RPC Interface Detected	
Level Risk:		0.0	
Service:	loc-srv	**CVE:**	-

Observation:
LSASS RPC Interface Detected.

Recommendation:
It is recommended to block the following ports at the network perimeter: 135/TCP,UDP,137/UDP, 138/TCP,UDP, 139/TCP,UDP 445/TCP,UDP, 593/TCP, 1025/TCP, 1026/TCP.

Description:
LSASS RPC Interface Detected.