Host Vulnerabilities Report

Hostname:	CITAD2_SG
IP Address:	10.11.14.18
Submit by:	admin
Generated Time:	Oct. 2, 2018, 9:23 a.m.

Table Of Contents

Host Detailed Information

Information

Submit by:		admin	
Created Date:		Sept. 10, 2018, 3:31 a.m.	
Updated Date:		Sept. 10, 2018, 3:31 a.m.	
Hostname:	CITAD2_SG	**Ip Address:**	10.11.14.18
OS:	Windows Server 2003 **	**Version:**	NA#

Description:
NA#

Running Service

Service	Network Port	Description
loc-srv	135	
vnc	5900	
http	80	
oracle-tns	1521	
mstaskremo	1026	
unknown	1027	
http-alt	8080	
ftp	21	
netbios-ns	137	
oracle-em2	1754	
amiganetfs	2100	

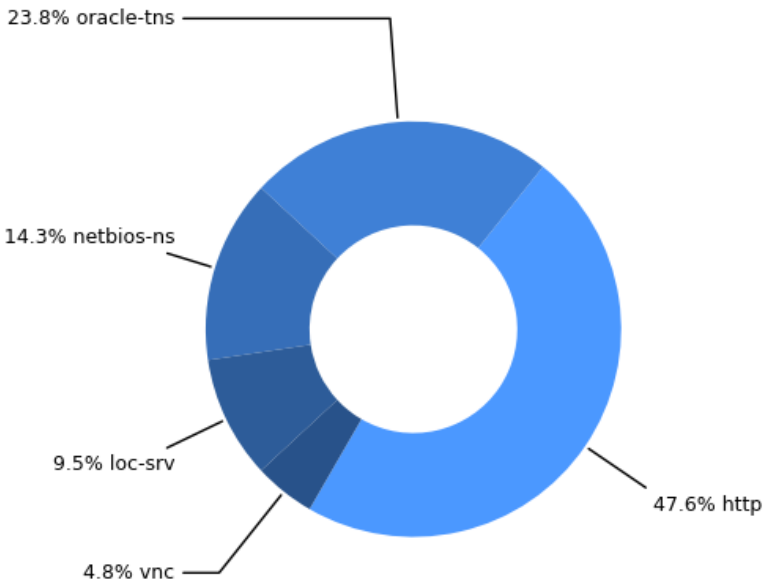
Table 1: Running Services of Host

Vulnerabilities

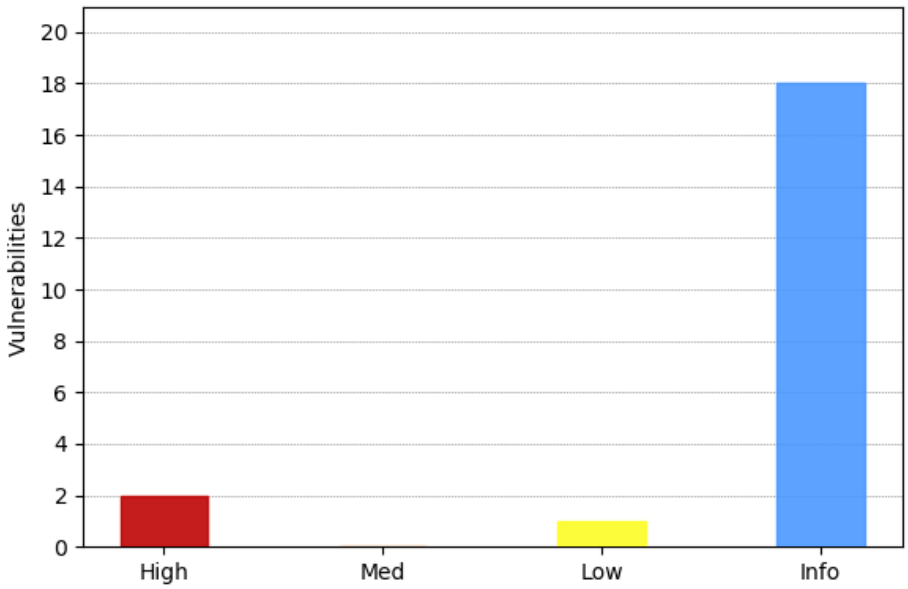
Overview

In this section, this report contains overview information that includes statistics by running services (in graph-1) and current categorized vulnerabilities (in graph-2) 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.



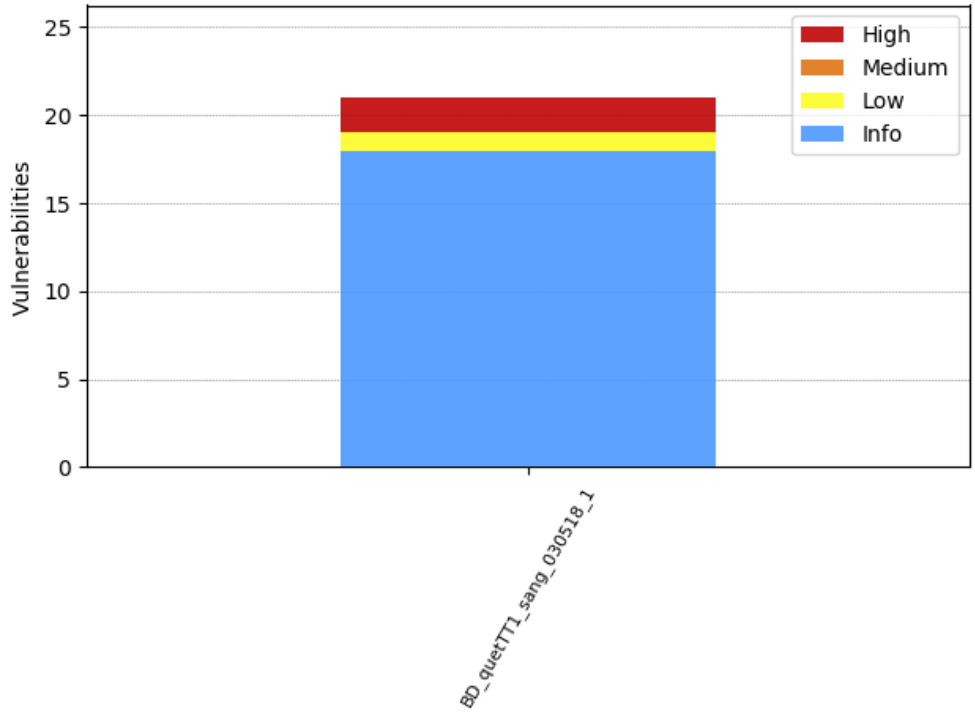
Graph 1: Vulnerabilities statistic by services



Graph 2: Current Vulnerabilities of Host

Scan History

In this section, the report contains scan history of host. It includes scan frequency and brief information of involved scan tasks.



Graph 3: Scan History Statistic of Host

Scan History:

Scan Task	Start Time	Finished Time	Vulnerabilities			
			High	Med	Low	Info
BD_quetTT1_sang_030518_1	May 3, 2018, 4:30 a.m.	May 3, 2018, 5:38 a.m.	2	0	1	18

Table 2: Scan History of Host

Current Vulnerabilities In Detail

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 TNS Listener Anonymous Access Allowed

Vulnerbility:		Oracle TNS Listener Anonymous Access Allowed	
Level Risk:		7.0	
Service:	oracle-tns	**CVE:**	CVE-2002-0567

Observation:
Oracle is an enterprise level database which is available on many different platforms. A configuration vulnerability exists within the Oracle TNS Listener which allows remote unauthenticated access. The TNS Listener accepts a clients request and establishes a TNS (Transparent Network Substrate) data connection between the client and the service. A TNS connection allows clients and servers to communicate over a network via a common API, regardless of the network protocol used on either end (TCP/IP, IPX, etc). A default installation of the TNS listens on TCP port 1521An Oracle TNS Listener service has been detected on the host with login security disabled (SECURITY=OFF).

Recommendation:
McAfee is currently unaware of a vendor-supplied patch or update (2016-12-16).It is recommended to only allow certain IP's or subnet ranges to access the TNS listener. This can be done by adding a rule in the firewall. We also recommend that you enable a password for the TNS listener within Oracle.

Description:
An Oracle TNS Listener service has been detected on the host with login security disabled (SECURITY=OFF).

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 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 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.

Oracle Database Server Version Below 10.1 Detected

Vulnerbility: Oracle Database Server Version Below 10.1 Detected
Level Risk: 0.0
Service: oracle-tns **CVE:** -

Observation:
Oracle Database is a widely used relational database management system. An obsolete version of Oracle Database was detected on the host.

Recommendation:
Upgrade the Oracle Database to the latest version from the following location: http://www.oracle.com

Description:
An obsolete version of Oracle Database 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.

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.

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 information. Workaround: 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 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 platform. Microsoft 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.

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 platform. Microsoft 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.

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.

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.

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.

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.

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 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.

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.

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.

Oracle Database Server Listener Unrestricted Access Detected

Vulnerbility: Oracle Database Server Listener Unrestricted Access Detected
Level Risk: 0.0
Service: oracle-tns **CVE:** -

Observation:
Oracle Database is a widely used relational database management system. Unrestricted access to Oracle Database TNS Listener was detected on the host.

Recommendation:
Ensure that Oracle Database Listener complies with organizational policy.

Description:
Unrestricted access to Oracle Database TNS Listener was detected on the host.

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.