Vulnerabilities
MANAGEMENT

# Host Vulnerabilities Report

| | |
|---|---|
| Hostname: | CI-CAPP-PR-Q3 |
| IP Address: | 10.1.178.17 |
| Submit by: | tuan.nt01 |
| Generated Time: | Oct. 9, 2018, 2:47 p.m. |

# Table Of Contents

# Host Detailed Information

## Information

| | | | |
|---|---|---|---|
| **Submit by:** | | admin | |
| **Created Date:** | | Sept. 10, 2018, 3:33 a.m. | |
| **Updated Date:** | | Sept. 10, 2018, 3:33 a.m. | |
| **Hostname:** | CI-CAPP-PR-Q3 | **Ip Address:** | 10.1.178.17 |
| **OS:** | Windows Server 2008 R2 Enterprise (Service Pack 1) | **Version:** | NA# |

**Description:**
NA#

## Running Service

| Service | Network Port | Description |
|---|---|---|
| loc-srv | 135 | |
| netbios-ssn | 139 | |
| microsoft-ds | 445 | |
| vnc | 5900 | |
| unknown | 49153 | |
| unknown | 49154 | |
| http | 80 | |
| unknown | 49155 | |
| unknown | 49152 | |

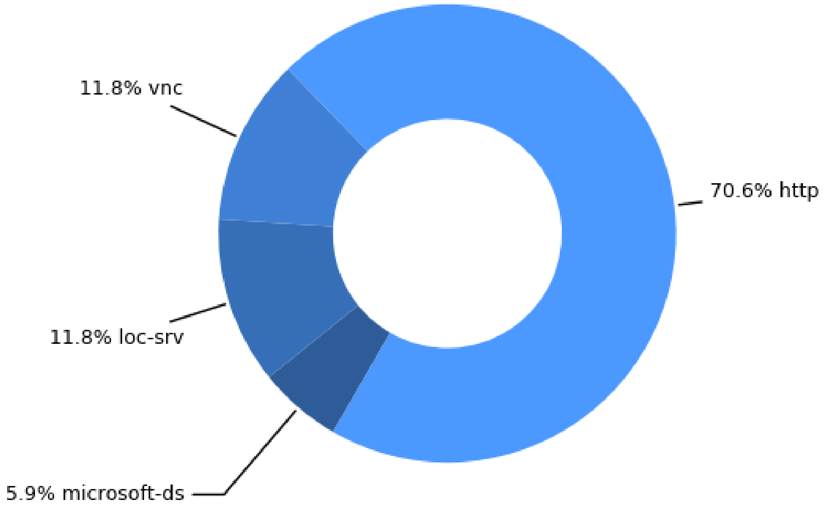
**Table 1:** Running Services of Host

# Vulnerabilities

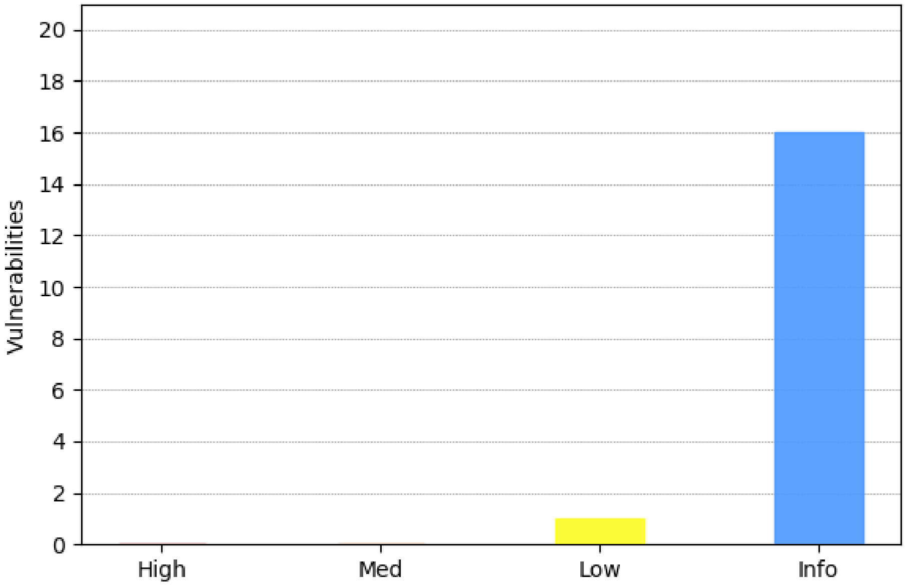
## Overview

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.



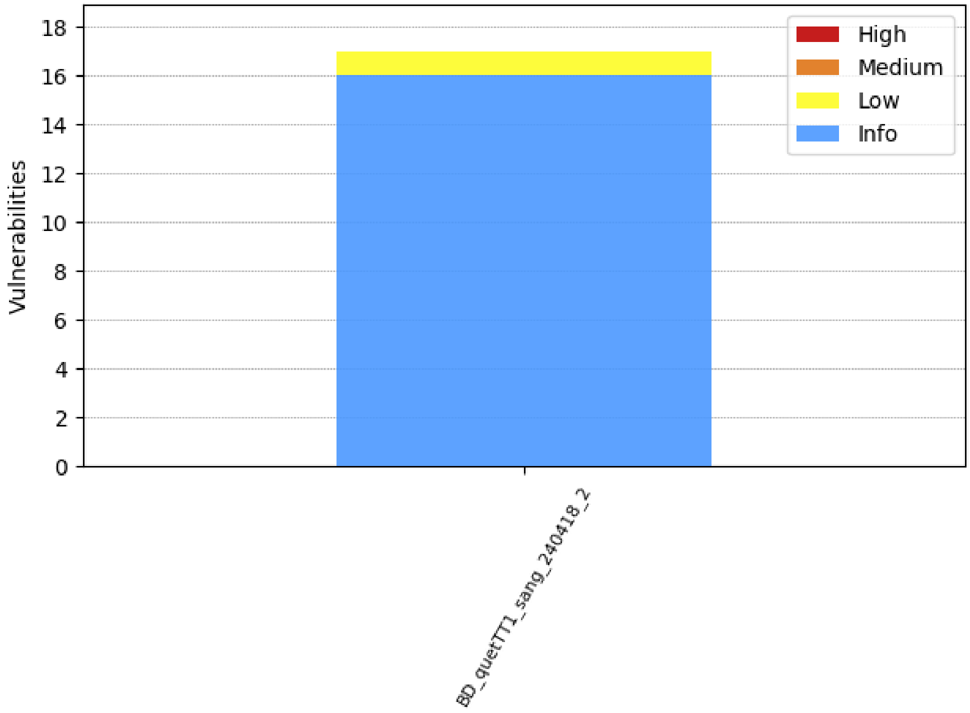
**Graph 1:** Vulnerabilities statistic by services



**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_240418_2 | April 24, 2018, 4:30 a.m. | April 24, 2018, 5:58 a.m. | 0 | 0 | 1 | 16 |

**Table 2:** Scan History of Host

# Current Vulnerabilities In Detail

## 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 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.

## VNC Server Security Type Detected

| | | | |
|---|---|---|---|
| **Vulnerbility:** | | VNC Server Security Type Detected | |
| **Level Risk:** | | 0.0 | |
| **Service:** | vnc | **CVE:** | - |

**Observation:**
VNC server is used to interact with desktop applications across any network.A VNC server security type supported was detected on the host.

**Recommendation:**
Ensure that the VNC server complies with organizational policy.

**Description:**
A VNC server security type supported was detected 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.

## 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.

## 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 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.

## 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.

## 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.

## 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 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.

## 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.

## 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 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 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.

## 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.