



Vulnerability Scan




















22 June 2016 at 10:29

URL : <http://www.rbpsoftwaresolutions.com>

Summary: 12 vulnerabilities found

HIGH 1 **MED** 6 **LOW** 5 **INFO** 26

Name	Vulnerability
Reflected Cross-Site Scripting (XSS) Vulnerabilities	
Login Form Is Not Submitted Via HTTPS	
Slow HTTP headers vulnerability	
Slow HTTP POST vulnerability	
Sensitive form field has not disabled autocomplete	
Unencoded characters	
Potential TCP Backdoor	
Windows Remote Desktop Protocol Weak Encryption Method Allowed	
SSL/TLS use of weak RC4 cipher	
SSL Certificate - Subject Common Name Does Not Match Server FQDN	
SSL Certificate - Signature Verification Failed Vulnerability	
Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure	
Server accepts unnecessarily large POST request body	INFO
Server Returns HTTP 500 Message For Request	INFO
Exhaustive Web Testing Skipped	INFO
Remote Access or Management Service Detected	INFO
Operating System Detected	INFO
Host Uptime Based on TCP TimeStamp Option	INFO
Firewall Detected	INFO

	Open TCP Services List	INFO
	Internet Service Provider	INFO
	TLS Secure Renegotiation Extension Support Information	INFO
	SSL Session Caching Information	INFO
	SSL Certificate - Information	INFO
	Host Scan Time	INFO
	Target Network Information	INFO
	Degree of Randomness of TCP Initial Sequence Numbers	INFO
	SSL Certificate will expire within next six months	INFO
	Default Web Page	INFO
	Traceroute	INFO
	Default Web Page	INFO
	IP ID Values Randomness	INFO
	Web Server Supports HTTP Request Pipelining	INFO
	DNS Host Name	INFO
	SSL Server Information Retrieval	INFO
	Host Names Found	INFO
	Web Server Supports HTTP Request Pipelining	INFO
	Microsoft Windows Network Level Authentication Disabled	INFO

Detailed results

Type: **Web Application**



Reflected Cross-Site Scripting (XSS) Vulnerabilities

QID: 150001

CVSS Base: 4.3

Category: Web Application

Port: -

CVEID: -

Threat:

XSS vulnerabilities occur when the Web application echoes user-supplied data in an

HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Impact:

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

Solution:

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

Results:

```
null -- q.ie.name")); var inen="" var insb="" if(inpr>0){ var
iqen=gebi("inq.ie.show").checked; var iqsb=gdv("inq.ie.subdesc"); }
divtedit("/inquiry-edit-accept?id="+"">qss
a=X144373548Y1Z>"+&row="+174+"&propid="+inpr+"&name="+iqna+"&enabled="
+iqen+"&subdesc="+iqsb,"inquiries-table","'>qss
a=X144373548Y1Z>,"inquiry-edit","inq-tr-">qss
a=X144373548Y1Z>");cancelBubble(event); '> Save</button> <button
onc,null -- inq.ie.name")); var inen="" var insb="" if(inpr>0){ var
iqen=gebi("inq.ie.show").checked; var iqsb=gdv("inq.ie.subdesc"); }
divtedit("/inquiry-edit-accept?id="+"">qss `;!--=&
{()}>"+&row="+174+"&propid="+inpr+"&name="+iqna+"&enabled="+iqen+"&sub
desc="+iqsb,"inquiries-table","'>qss `;!--=&{()}>,"inquiry-
edit","inq-tr-">qss `;!--=&{()}>");cancelBubble(event); '>
Save</button> <button onclick='cd("
```



Login Form Is Not Submitted Via HTTPS

QID: 150053

CVSS Base: 8.5

Category: Web Application

Port: -

CVEID: -

Threat:

The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

Impact:

Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

Solution:

Change the login form's action to submit via HTTPS.

Results:

http://www.rbpssoftwaresolutions.com/ -- comment: Parent URL of Login Form is : http://www.rbpssoftwaresolutions.com/ Login Form Is Not Submitted Via HTTPS



Slow HTTP headers vulnerability

QID: 150079

CVSS Base: 6.8

Category: Web Application

Port: -

CVEID: -

Threat:

The web application is possibly vulnerable to "slow HTTP headers" Denial of Service (DoS) attack. This is an application-level DoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection. One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever. More information can be found at the [Slowloris HTTP DoS](#).

Impact:

All other services remain intact but the web server itself becomes completely inaccessible.

Solution:

Server-specific recommendations can be found [here](#). Countermeasures for Apache are described [here](#). Easy to use tool for intrusive testing is available [here](#).

Results:

`http://www.rbpsoftwareolutions.com/support? -- Vulnerable to slow HTTP headers attack Server resets timeout after accepting header data from peer.`



Slow HTTP POST vulnerability

QID: 150085

CVSS Base: 6.8

Category: Web Application

Port: -

CVEID: -

Threat:

The web application is possibly vulnerable to a "slow HTTP POST" Denial of Service (DoS) attack. This is an application-level DoS that consumes server resources by maintaining open connections for an extended period of time by slowly sending traffic to the server. If the server maintains too many connections open at once, then it may not be able to respond to new, legitimate connections. Unlike bandwidth-consumption DoS attacks, the "slow" attack does not require a large amount of traffic to be sent to the server -- only that the client is able to maintain open connections for several minutes at a time. The attack holds server connections open by sending properly crafted HTTP POST headers that contain a Content-Length header with a large value to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources. By waiting for the complete request body, the server is helping clients with slow or intermittent connections to complete requests, but is also exposing itself to abuse.

Further information can be found under [BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf](#).

Impact:

All other services remain intact but the web server itself becomes inaccessible.

Solution:

Solution would be server-specific, but general recommendations are: - to limit the size of

the acceptable request to each form requirements - establish minimal acceptable speed rate - establish absolute request timeout for connection with POST request Server-specific details can be found [here](#) . A tool that demonstrates this vulnerability in a more intrusive manner is available [here](#) .

Results:

`http://www.rbpsoftware resolutions.com/support? -- Vulnerable to slow HTTP POST attack Server resets timeout after accepting request data from peer.`

**Sensitive form field has not disabled autocomplete****QID:** 150112**CVSS Base:****Category:** Web Application**Port:** -**CVEID:** -**Threat:**

An HTML form that collects sensitive information (such as a password field) does not prevent the browser from prompting the user to save the populated values for later reuse. Stored credentials should not be available to anyone but their owner.

Impact:

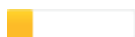
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user. For example, if a browser saves the login name and password for a form, then anyone with access to the browser may submit the form and authenticate to the site without having to know the victim's password.

Solution:

Add the following attribute to the form or input element: `autocomplete="off"` This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Results:

`http://www.rbpsoftware resolutions.com/ -- Form field does not set autocomplete="off".`

**Unencoded characters****QID:** 150084**CVSS Base:****Category:** Web Application**Port:** -**CVEID:** -**Threat:**

The web application reflects potentially dangerous characters such as single quotes, double quotes, and angle brackets. These characters are commonly used for HTML injection attacks such as cross-site scripting (XSS).

Impact:

No exploit was determined for these reflected characters. The input parameter should be manually analyzed to verify that no other characters can be injected that would lead to an HTML injection (XSS) vulnerability.

Solution:

Review the reflected characters to ensure that they are properly handled as defined by the web application's coding practice. Typical solutions are to apply HTML encoding or percent encoding to the characters depending on where they are placed in the HTML. For example, a double quote might be encoded as `"` when displayed in a text node, but as `%22` when placed in the value of an href attribute.

Results:

`null -- comment: A significant portion of the XSS test payload`

```

appeared in the web page, but the page's DOM was not modified as
expected for a successful exploit. This result should be manually
verified to determine its accuracy. name")); var inen="" var insb=""
if(inpr>0){ var iqen=gebi("inq.ie.show").checked; var
iqsb=gdv("inq.ie.subdesc"); } divtedit("/inquiry-edit-accept?id="+"">
<<SCRIPT
a=2>qss=7;//<</SCRIPT>+"&row="+174+"&propid="+inpr+"&name="+iqna+"&ena
bled="+iqen+"&subdesc="+iqsb,"inquiries-table","'><<SCRIPT
a=2>qss=7;//<</SCRIPT>,"inquiry-edit","inq-tr-'><<SCRIPT
a=2>qss=7;//<</SCRIPT>");cancelBubble(event); '> Save</

```

Type: Vulnerability



Potential TCP Backdoor

QID: 1004

CVSS Base: 4.9

Category: Backdoors and trojan horses

Port: 0

CVEID: -

Threat:

There are known backdoors that use specific port numbers. At least one of these ports was found open on this host. This may indicate the presence of a backdoor; however, it's also possible that this port is being used by a legitimate service, such as a Unix or Windows RPC.

Impact:

If a backdoor is present on your system, then unauthorized users can log in to your system undetected, execute unauthorized commands, and leave the host vulnerable to other unauthorized users. Malicious users may also use your host to access other hosts and perform a coordinated Denial of Service attack.

Some well-known backdoors are "BackOrifice", "Netbus" and "Netspy". You should be able to find more information on these backdoors on the [CERT Coordination Center's Web site \(www.cert.org\)](http://www.cert.org).

Solution:

Call a security specialist and test the host for backdoors. If a backdoor is found, then the host may need to be re-installed.

Results:

The tcp port 1999 is open, it may indicate the presence of a "tcp-id-port" backdoor.



Windows Remote Desktop Protocol Weak Encryption Method Allowed

QID: 90882

CVSS Base: 4.7

Category: Windows

Port: 3389

CVEID: -

Threat:

Remote Desktop Protocol is a protocol by which Terminal Service provides desktop level access to a remote user. It can be used to remotely log in and interact with a Windows machine.

Since RDP transfers sensitive information about the user and the system, it can be configured to use encryption to provide privacy and integrity for its sessions. It is possible to configure RDP to use encryption algorithms that are considered insecure, such as RC4 40bit and RC4 56 bit.

Impact:

If an attacker has access to the network traffic with RDP sessions using weak encryption methods it's possible to bruteforce the encryption parameters and compromise privacy of the RDP session.

Solution:

RDP needs to be configured to use strong encryption methods or use SSL as the privacy and integrity provider.

To configure RDP encryption methods 'Terminal Services Configuration' or 'Remote Desktop Session Host Configuration' snap-in can be launched in mmc.exe.

In 'Terminal Services Configuration' or 'Remote Desktop Session Host Configuration' properties dialog box General tab for the Encryption Level 'High' should be selected.

On Windows XP the RDP configuration can be found under Computer Configuration\Administrative Templates\Windows Components\Terminal Services and User Configuration\Administrative Templates\Windows Components\Terminal Services. Under Encryption and Security item, double click on 'Set client connection encryption level' and enable the policy and select high for the 'Encryption level'.

For more details on configuration on 2008 R2 systems see [Configure Server Authentication and Encryption Levels](#).

For more detail on disabling RC4 see [Microsoft Update for Disabling RC4](#).

For details on supporting TLS 1.1 and TLS1.2 for Remote Desktop Services see [Update to add RDS support for TLS 1.1 and TLS 1.2 in Windows 7 or Windows Server 2008 R2](#).

Results:

RDP Supported Encryption methods: RC4(40 bit),RC4(56 bit)

**SSL/TLS use of weak RC4 cipher**

QID: 38601

CVSS Base: 4.3

Category: General remote services

Port: 3389

CVEID: [CVE-2013-2566](#), [CVE-2015-2808](#)

Threat:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features. SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

Impact:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from ciphertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

Solution:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

Results:

TLSv1.0 with RC4 ciphers is supported

Type: **Vulnerability****SSL Certificate - Subject Common Name Does Not Match Server FQDN****QID:** 38170**CVSS Base:** 2.6**Category:** General remote services**Port:** 3389**CVEID:** -**Threat:**

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

Impact:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

Solution:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

Results:

Certificate #0 CN=WIN-80T2VA2GMCP (WIN-80T2VA2GMCP) doesn't resolve

**SSL Certificate - Signature Verification Failed Vulnerability****QID:** 38173**CVSS Base:** 3.7**Category:** General remote services**Port:** 3389**CVEID:** -**Threat:**

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

Impact:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

Solution:

Please install a server certificate signed by a trusted third-party Certificate Authority.

Results:

Certificate #0 CN=WIN-80T2VA2GMCP unable to get local issuer

certificate

Type: **Vulnerability****Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure****QID:** 90250**CVSS Base:** 6.7**Category:** Windows**Port:** 0**CVEID:** [CVE-2005-1794](#)**Threat:**

Microsoft Windows Remote Desktop Protocol is affected by a private key disclosure vulnerability.

When an RDP client initiates a session with an RDP server, the server responds with a server certificate containing an RSA public key and its digital signature. The client decrypts the signature using the server's public key and compares the result with the hash of the new public key received from the server to verify the identity of the server.

The vulnerability presents itself because a private key that is used to sign the Terminal Server public key is hardcoded in "mstlsapi.dll". A subroutine of the "TLSInit" API dynamically creates, uses and de-allocates this key.

Impact:

Successful exploitation can allow the attacker to disclose the key and calculate a valid signature to carry out man in the middle attacks. An attacker could therefore cause the client to connect to a server under their control and send the client a public key to which they possess the private key.

Solution:

There are no vendor-supplied solutions available at this time.

Workarounds:

- As there is no patch, this vulnerability should be mitigated by using some semblance of network filtering (e.g., firewalling RDP off from the open Internet).

For Windows Server 2003, the security of Terminal Server can be enhanced by configuring Terminal Services connections to use Transport Layer Security (TLS) 1.0 for server authentication, and to encrypt terminal server communications. Please refer to [cc782610](#) to obtain additional details.

Results:

Detected service win_remote_desktop and os WINDOWS VISTA / WINDOWS 2008 / WINDOWS 7 / WINDOWS 2012 / WINDOWS 8 / WINDOWS 10

Type: **Web Application****INFO****Server accepts unnecessarily large POST request body****QID:** 150086**CVSS Base:****Category:** Web Application**Port:** -**CVEID:** -**Threat:**

Web application scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the [here](#)

Impact:

Could result in successful application level (Layer 7) DDoS attack.

Solution:

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found [here](#).

Results:

http://www.rbpsoftwaresolutions.com -- Server responded 200 to unnecessarily large random request body(over 64 KB) for URL http://www.rbpsoftwaresolutions.com/support?, significantly increasing attacker's chances to prolong slow HTTP POST attack.

INFO**Server Returns HTTP 500 Message For Request****QID:** 150042**CVSS Base:****Category:** Web Application**Port:** -**CVEID:** -**Threat:**

During the scanning engine's crawl phase, the Web server responded with an HTTP 500 message for each link listed below. The HTTP 500 message indicates a server error.

Impact:

The presence of an HTTP 500 error during the crawl phase indicates that some problem exists in the Web site that will be encountered during normal usage of the Web application.

Solution:

Review each link to determine why the server encountered an error when responding to the link.

Results:

http://www.rbpsoftwaresolutions.com --
http://www.rbpsoftwaresolutions.com/add-associate?
http://www.rbpsoftwaresolutions.com/add-group?
http://www.rbpsoftwaresolutions.com/department-add-accept?name=
http://www.rbpsoftwaresolutions.com/add-associate?&rnd=29899
http://www.rbpsoftwaresolutions.com/edit-inquiry?id=174&row=174
http://www.rbpsoftwaresolutions.com/add-associate?&rnd=39981
http://www.rbpsoftwaresolutions.com/add-associate?&rnd=83139
http://www.rbpsoftwaresolutions.com/add-associate?&rnd=43107
http://www.rbpsoftwaresolutions.com/add-group?&rnd=4500
http://www.rbpsoftwaresolutions.com/add-group?&rnd=1611
http://www.rbpsoftwaresolutions.com/add-associate?&rnd=87551
http://www.rbpsoftwaresolutions.com/add-group?&rnd=23048

Type: Vulnerability**INFO****Exhaustive Web Testing Skipped****QID:** 86718**CVSS Base:****Category:** Web server**Port:** 80**CVEID:** -**Threat:**

The service aborted the scanning of the Web server before completion, since the Web server stopped responding to HTTP requests during the course of scanning. The service attempted to reconnect to the Web server two minutes later and found it responsive again. However, the service has chosen to stop further scanning of the Web server to avoid possible interruption of the Web service.

Impact:

Since the service did not complete scanning this host, not all vulnerability tests were

completed. It's possible that not all vulnerabilities were detected for this host.

Solution:

There may have been a number of conditions that contributed to this issue. The following is a partial list of possibilities that should be investigated:

- The Web server may have reached its connection limit.
- The Web server (or an intervening network device) may have been purposefully throttling connections (e.g. mod_throttle for Apache).
- The Web server (or an intervening network device) may contain an undisclosed Denial of Service condition that was triggered by the scan traffic.
- The Web server (or an intervening network device) may have experienced a degradation of performance due to high load (e.g. via scanning multiple virtual IPs on the same physical host).
- The scan traffic may have been traversing a network segment with limited bandwidth capacity.
- An Intrusion Prevention System, reactive firewall, or similar device may have detected and blocked the scan traffic.

This issue may possibly be mitigated by modifying the scan performance settings in your option profile before scanning the host again.

Results:

The web server stopped responding to 4 consecutive HTTP requests 2 minutes ago. Although it resumed responding to a new HTTP request but the service had terminated further scanning of the web server to avoid interrupting the web server's normal functionality and a prolonged scanning time.

INFO**Remote Access or Management Service Detected****QID:** 42017**CVSS Base:****Category:** General remote services**Port:** 0**CVEID:** -**Threat:**

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

Impact:

Consequences vary by the type of attack.

Solution:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

Results:

Service name: Remote Desktop on TCP port 3389.

INFO**Operating System Detected****QID:** 45017**CVSS Base:****Category:** Information gathering**Port:** 0**CVEID:** -**Threat:**

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint:** The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS:** Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info:** PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP:** The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

Impact:

Not applicable

Solution:

Not applicable

Results:

```
#table cols="3" Operating_System Technique ID
Windows_Vista/_Windows_2008/_Windows_7/_Windows_2012/_Windows_8/_
Windows_10 TCP/IP_Fingerprint U3414:80
```

INFO

Host Uptime Based on TCP TimeStamp Option

QID: 82063

CVSS Base:

Category: TCP/IP

Port: 0

CVEID: -

Threat:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

Impact:

N/A

Solution:

N/A

Results:

Based on TCP timestamps obtained via port 80, the host's uptime is 162 days, 19 hours, and 35 minutes. The TCP timestamps from the host are in units of 10 milliseconds.

INFO

Firewall Detected**QID:** 34011**CVSS Base:****Category:** Firewall**Port:** 0**CVEID:** -**Threat:**

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

Impact:**Solution:****Results:**

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 443, 445. Listed below are the ports filtered by the firewall. No response has been received when any of these ports is probed. 1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-223,242-246,256-265, 280-282,309,311,318,322-325,344-351,363,369-581,587,592-593,598,600,606-620, 624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,740-742,744, 747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,900-901, 911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,1109-1112, 1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,1241,1243, 1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,1776-1815, 1818-1824,1900,1902-1909,1911-1920,1944-1951,1973,1981,1985-1998,2001-2028, 2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more. We have omitted from this list 702 higher ports to keep the report size manageable.

INFO

Open TCP Services List**QID:** 82023**CVSS Base:****Category:** TCP/IP**Port:** 0**CVEID:** -**Threat:**

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

Impact:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

Solution:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the [CERT Web site](#).

Results:

```
#table cols="5" Port IANA_Assigned_Ports/Services Description
Service_Detected OS_On_Redirected_Port 80 www World_Wide_Web_HTTP
http_ _ 1901 fjicl-tep-a Fujitsu_ICL_Terminal_Emulator_Program_A
unknown_ _ 1999 tcp-id-port
cisco_identification_port_Transcout_1.1+_1.2_backdoor unknown_ _ 2000
openwindow callbook unknown_ _ 3389 ms-wbt-server MS_WBT_Server
win_remote_desktop_over_ssl _ 8080 http-alt
```

HTTP_Alternate_(see_port_80) http_ _ 8081 unknown unknown http_ _

INFO**Internet Service Provider****QID:** 45005**CVSS Base:****Category:** Information gathering**Port:** 0**CVEID:** -**Threat:**

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

Impact:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

Solution:

N/A

Results:

The ISP network handle is: AMAZON-05 ISP Network description: Amazon.com, Inc.

INFO**TLS Secure Renegotiation Extension Support Information****QID:** 42350**CVSS Base:****Category:** General remote services**Port:** 3389**CVEID:** -**Threat:**

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact:

N/A

Solution:

N/A

Results:

TLS Secure Renegotiation Extension Status: supported.

INFO**SSL Session Caching Information****QID:** 38291**CVSS Base:****Category:** General remote services**Port:** 3389**CVEID:** -

Threat:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters. This test determines if SSL session caching is enabled on the host.

Impact:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution:**Results:**

TLSv1 session caching is disabled on the target.

INFO**SSL Certificate - Information****QID:** 86002**CVSS Base:****Category:** Web server**Port:** 3389**CVEID:** -**Threat:****Impact:****Solution:****Results:**

```
#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2)
(0)Serial_Number _64:bc:3c:44:14:1f:5b:bb:40:54:98:ed:d8:82:bd:51_
(0)Signature_Algorithm sha1WithRSAEncryption (0)ISSUER_NAME _
commonName WIN-80T2VA2GMCP (0)SUBJECT_NAME _ commonName WIN-
80T2VA2GMCP (0)Valid_From Jun_6_17:56:50_2016_GMT (0)Valid_Till
Dec_6_17:56:50_2016_GMT (0)Public_Key_Algorithm rsaEncryption
(0)RSA_Public_Key (2048_bit) (0) _Public-Key:_(2048_bit) (0) _Modulus:
(0) _00:a2:73:37:18:f1:e9:1a:18:9d:b1:7a:22:25:2a: (0)
_d2:b4:e8:dd:93:f0:5e:0d:98:b4:1a:49:b7:0a:76: (0)
_98:dc:e0:e5:00:cc:ba:d5:18:5b:2b:d7:d8:6b:ff: (0)
_c3:8e:eb:ab:ac:a2:55:6b:2b:ca:6f:e8:67:bb:84: (0)
_e9:85:3e:d9:79:4a:f7:29:e1:c7:d8:ea:dd:1b:f4: (0)
_d9:7f:04:e5:3c:fc:40:68:34:d3:4e:61:bd:41:f6: (0)
_33:ed:91:92:e4:6c:ee:6e:e9:83:b6:40:c5:70:5b: (0)
_48:5a:22:67:95:3f:25:02:a6:7e:80:4c:66:b5:84: (0)
_ee:e2:1b:0e:ba:b9:c1:97:a8:29:5a:8b:99:71:3a: (0)
_f4:da:bf:28:72:ee:e8:60:fd:7a:be:18:3e:f5:ad: (0)
_83:02:77:ea:98:b9:26:dd:bf:31:d4:7f:8b:93:00: (0)
_b5:e5:33:7a:b2:70:3c:af:01:6d:26:28:2e:12:9e: (0)
_dc:26:77:42:eb:4d:27:86:11:4f:05:ee:96:18:36: (0)
_ac:fb:38:10:2a:5c:19:57:bd:6a:80:06:66:08:a0: (0)
_cb:be:5d:7c:00:42:02:16:5e:91:53:87:0d:be:f3: (0)
_3a:6b:f1:65:5d:38:39:0a:36:1e:31:60:46:54:77: (0)
_5b:12:d9:f8:78:f4:db:4f:58:18:64:c9:13:48:29: (0) _5f:a7 (0)
_Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _
(0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication
(0)X509v3_Key_Usage _Key_Encipherment,_Data_Encipherment (0)Signature
(256_octets) (0) 5c:f4:53:70:93:99:f6:c7:7f:8f:fd:b1:c6:01:bb:a9 (0)
ca:58:6d:e1:22:42:0b:9e:01:74:3c:87:6d:a4:6d:fb (0)
c1:44:52:05:63:eb:2d:fe:0c:68:75:bb:aa:0a:0f:21 (0)
ec:c6:5e:99:67:6c:cf:89:55:66:c2:dd:c6:48:1b:8c (0)
1b:27:d2:d1:f8:36:b6:e2:b2:f6:a2:b5:5d:b1:50:7c (0)
df:de:39:87:30:f7:b0:04:c9:8f:d9:47:48:ba:72:8d (0)
a4:09:2b:33:38:f1:26:a3:6b:3b:3c:c0:d7:9a:19:a7 (0)
```

```
ec:c5:0a:9e:05:0f:f9:7a:48:99:87:07:d8:03:36:0c (0)
20:4c:40:33:fb:62:1b:dc:a6:ec:6e:0f:86:b9:e3:70 (0)
b5:25:4f:67:86:1b:e4:b3:02:a4:8f:be:55:b2:d2:e7 (0)
fe:22:cc:40:84:87:cf:e6:79:db:09:3a:58:73:1e:aa (0)
63:06:d0:31:67:e4:bd:fd:a3:b4:56:2f:36:f1:68:a8 (0)
4c:fc:2d:cc:98:f0:bc:74:d7:d8:17:22:13:a7:a8:f3 (0)
27:4c:b7:01:cd:ee:9e:8e:9c:b7:93:ad:59:86:5a:87 (0)
05:12:19:18:64:76:8e:6e:ec:83:20:3e:d0:6a:6e:4e (0)
4e:f7:50:87:79:38:3e:74:91:5f:e8:b0:88:6c:44:45
```

INFO**Host Scan Time****QID: 45038****CVSS Base:****Category: Information gathering****Port: 0****CVEID: -****Threat:**

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

Impact:

N/A

Solution:

N/A

Results:

Scan duration: 819 seconds Start time: Wed, Jun 22 2016, 17:10:04 GMT

End time: Wed, Jun 22 2016, 17:23:43 GMT

INFO**Target Network Information****QID: 45004****CVSS Base:****Category: Information gathering****Port: 0****CVEID: -****Threat:**

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

Impact:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

Solution:

N/A

Results:

The network handle is: AMAZON-2011L Network description: Amazon Technologies Inc.

INFO**Degree of Randomness of TCP Initial Sequence Numbers****QID:** 82045**CVSS Base:****Category:** TCP/IP**Port:** 0**CVEID:** -**Threat:**

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

Impact:

N/A

Solution:

N/A

Results:

Average change between subsequent TCP initial sequence numbers is 1185834898 with a standard deviation of 626677080. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5169 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

INFO**SSL Certificate will expire within next six months****QID:** 38600**CVSS Base:****Category:** General remote services**Port:** 3389**CVEID:** -**Threat:**

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

Impact:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

Solution:

Contact the certificate authority that signed your certificate to arrange for a renewal.

Results:

Certificate #0 CN=WIN-80T2VA2GMCP The certificate will expire within six months: Dec 6 17:56:50 2016 GMT

INFO**Default Web Page****QID:** 12230**CVSS Base:****Category:** CGI**Port:** 8081**CVEID:** -

Threat:

The Result section displays the default Web page for the Web server.

Impact:

N/A

Solution:

N/A

Results:

Cannot GET /

INFO**Traceroute**

QID: 45006

CVSS Base:

Category: Information gathering

Port: 0

CVEID: -

Threat:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

Impact:**Solution:****Results:**

```
#table cols="4" Hops IP Round_Trip_Time Probe 1 64.39.103.251 0.41ms
ICMP 2 216.35.14.45 0.77ms ICMP 3 216.33.4.73 0.50ms ICMP 4
206.28.101.97 0.92ms ICMP 5 63.235.40.205 0.85ms ICMP 6 67.14.28.110
67.63ms ICMP 7 67.133.224.206 68.40ms ICMP 8 *.*.*.* 0.00ms Other 9
*.*.*.* 0.00ms Other 10 54.239.110.245 77.74ms ICMP 11 54.239.111.105
68.61ms ICMP 12 205.251.245.246 68.64ms ICMP 13 *.*.*.* 0.00ms Other
14 *.*.*.* 0.00ms Other 15 *.*.*.* 0.00ms Other 16 *.*.*.* 0.00ms
Other 17 *.*.*.* 0.00ms Other 18 54.172.195.130 73.74ms TCP
```

INFO**Default Web Page**

QID: 12230

CVSS Base:

Category: CGI

Port: 8080

CVEID: -

Threat:

The Result section displays the default Web page for the Web server.

Impact:

N/A

Solution:

N/A

Results:

Cannot GET /

INFO**IP ID Values Randomness**

QID: 82046

CVSS Base:

Category: TCP/IP

Port: 0

CVEID: -

displayed in the RESULT section.

Impact:**Solution:****Results:**

```
#table IP_address Host_name 54.172.195.130
www.rbpssoftwaresolutions.com 54.172.195.130 ec2-54-172-195-
130.compute-1.amazonaws.com
```

INFO**SSL Server Information Retrieval****QID:** 38116**CVSS Base:****Category:** General remote services**Port:** 3389**CVEID:** -**Threat:**

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact:

N/A

Solution:

N/A

Results:

```
#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-
STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _
SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_ENABLED _ _ _ _ _
_ TLSv1_COMPRESSION_METHOD None _ _ _ RC4-MD5 RSA RSA MD5 RC4(128) _ _ _
_MEDIUM_ RC4-SHA RSA RSA SHA1 RC4(128) _MEDIUM_ DES-CBC3-SHA RSA RSA
SHA1 3DES(168) _HIGH_ AES128-SHA RSA RSA SHA1 AES(128) _MEDIUM_
AES256-SHA RSA RSA SHA1 AES(256) _HIGH_ ECDHE-RSA-AES128-SHA ECDH RSA
SHA1 AES(128) _MEDIUM_ ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256)
_HIGH_
```

INFO**Host Names Found****QID:** 45039**CVSS Base:****Category:** Information gathering**Port:** 0**CVEID:** -**Threat:**

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

Impact:

N/A

Solution:

N/A

Results:

```
#table cols="2" Host_Name Source www.rbpssoftwaresolutions.com User-
provided_DNS ec2-54-172-195-130.compute-1.amazonaws.com FQDN
```

INFO

Web Server Supports HTTP Request Pipelining**QID:** 86565**CVSS Base:****Category:** Web server**Port:** 8080**CVEID:** -**Threat:**

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

Impact:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

Solution:

N/A

Results:

```
GET / HTTP/1.1 Host:54.172.195.130:8080 GET /Q_Evasive/ HTTP/1.1
Host:54.172.195.130:8080 HTTP/1.1 404 Not Found X-Powered-By: Express
X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8
Content-Length: 13 Date: Wed, 22 Jun 2016 17:11:41 GMT Connection:
keep-alive Cannot GET / HTTP/1.1 404 Not Found X-Powered-By: Express
X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8
Content-Length: 23 Date: Wed, 22 Jun 2016 17:11:41 GMT Connection:
keep-alive Cannot GET /Q_Evasive/
```

INFO

Microsoft Windows Network Level Authentication Disabled**QID:** 90788**CVSS Base:****Category:** Windows**Port:** 0**CVEID:** -**Threat:**

Microsoft Windows Network Level Authentication (NLA) is an authentication method that enhances the security of a Remote Desktop Session Host server by requiring the user to be authenticated before a session is created.

The registry key for the Network Level Authentication (NLA) is disabled.

Network Level Authentication is supported on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2

Impact:

Enabling NLA can help protect the remote computer from malicious users and malicious software attacks.

Solution:

See Microsoft Knowledge Base Article [2671387](#) to use the automated Microsoft Fix it solution to enable this feature.

As a precaution, always test in a QA or rehearsal environment before rolling out to production.

Note: Client computers that do not support Credential Security Support Provider (CredSSP) protocol will not be able to access servers protected with Network Level Authentication. Windows XP does not support the CredSSP protocol by default.

Results:

QID: 90788 detected on port 3389 over TCP.

