

Payment Card Industry (PCI) Current Vulnerabilities Report

10/30/2020

IP Addresses

216.66.77.198

Detailed Results

216.66.77.198 (usw-s005.rsyntax.net,-)

Vulnerabilities Total

15

Security Risk

0.0


Information Gathered (15)

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 

QID: 42017

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/23/2019

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.

RESULT:


Service name: SSH on TCP port 22.

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82040
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2003

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol \geq 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

RESULT:


ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82046
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2006

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.


Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

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.

RESULT:


Average change between subsequent TCP initial sequence numbers is 1120211367 with a standard deviation of 536830223. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4999 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

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 (<http://www.cert.org>).

RESULT:


Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 6
 Category: Information gathering
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 01/03/2018

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:


IP address	Host name
216.66.77.198	usw-s005.rsync.net

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 45006
 Category: Information gathering
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 05/09/2003

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.

RESULT:

Hops	IP	Round Trip Time	Probe	Port
1	64.39.111.3	0.41ms	ICMP	
2	216.35.14.45	0.44ms	ICMP	
3	*.*.*	0.00ms	Other	22
4	67.14.43.82	3.91ms	ICMP	
5	67.14.34.214	4.74ms	ICMP	
6	4.68.73.45	5.42ms	ICMP	
7	4.69.219.61	5.02ms	ICMP	


8	65.19.191.117	5.57ms	ICMP
9	184.104.192.213	5.42ms	ICMP
10	184.105.213.158	5.99ms	ICMP
11	216.66.77.198	5.89ms	ICMP

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45004

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 08/15/2013

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.

RESULT:


The network handle is: HURRICANE-6
 Network description:
 Hurricane Electric LLC

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45005

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 09/27/2013

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.

RESULT:


The ISP network handle is: LVL-ORG-4-8
ISP Network description:
Level 3 Parent, LLC

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/26/2020

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.

RESULT:


Host Name	Source
usw-s005.rsnc.net	FQDN

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/17/2016

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.

RESULT:

Scan duration: 436 seconds

Start time: Thu, Oct 29 2020, 20:40:19 GMT


End time: Thu, Oct 29 2020, 20:47:35 GMT

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45426
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/24/2020

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

RESULT:


Protocol	Port	Time
TCP	22	0:02:05

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 04/21/2019

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).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 443, 445.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

1-21,23-381,383-2868,2870-6128,6130-61999,64001-65535

SSH daemon information retrieving

port 22/tcp

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

Severity: 1

QID: 38047

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/03/2018

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentication methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentication methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

RESULT:

SSH1 supported	no
SSH2 supported	yes

Supported key exchange algorithms for SSH2	curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256
Supported host key algorithms for SSH2	ssh-ed25519
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password, keyboard-interactive


SSH Banner

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38050

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 10/29/2020

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:

The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

SSH-2.0-OpenSSH_8.2-hpn14v15 FreeBSD-openssh-portable-8.2.p1_1,1

Report Legend

Payment Card Industry (PCI) Status






The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.




A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels




A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.



Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.




Severity	Level	Description
 LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
 MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.




Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
	1	Minimal Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2	Medium Intruders may be able to determine the operating system running on the host, and view banner versions.
	3	Serious Intruders may be able to detect highly sensitive data, such as global system user lists.

Payment Card Industry (PCI) Current Vulnerabilities Report

10/30/2020

IP Addresses

216.66.77.198

Detailed Results

216.66.77.198 (usw-s005.rsinc.net,-)

Vulnerabilities Total

15

Security Risk

0.0


Information Gathered (15)

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 

QID: 42017

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/23/2019

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.

RESULT:


Service name: SSH on TCP port 22.

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82040
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2003

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol \geq 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

RESULT:


ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82046
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2006

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.


Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

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.

RESULT:


Average change between subsequent TCP initial sequence numbers is 1120211367 with a standard deviation of 536830223. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4999 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

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 (<http://www.cert.org>).

RESULT:


Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 6
 Category: Information gathering
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 01/03/2018

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:


IP address	Host name
216.66.77.198	usw-s005.rsync.net

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 45006
 Category: Information gathering
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 05/09/2003

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.

RESULT:

Hops	IP	Round Trip Time	Probe	Port
1	64.39.111.3	0.41ms	ICMP	
2	216.35.14.45	0.44ms	ICMP	
3	*.*.*	0.00ms	Other	22
4	67.14.43.82	3.91ms	ICMP	
5	67.14.34.214	4.74ms	ICMP	
6	4.68.73.45	5.42ms	ICMP	
7	4.69.219.61	5.02ms	ICMP	


8	65.19.191.117	5.57ms	ICMP
9	184.104.192.213	5.42ms	ICMP
10	184.105.213.158	5.99ms	ICMP
11	216.66.77.198	5.89ms	ICMP

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45004

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 08/15/2013

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.

RESULT:


The network handle is: HURRICANE-6
 Network description:
 Hurricane Electric LLC

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45005

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 09/27/2013

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.

RESULT:


The ISP network handle is: LVL3-ORG-4-8
ISP Network description:
Level 3 Parent, LLC

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/26/2020

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.

RESULT:


Host Name	Source
usw-s005.rsinc.net	FQDN

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/17/2016

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.

RESULT:

Scan duration: 436 seconds

Start time: Thu, Oct 29 2020, 20:40:19 GMT


End time: Thu, Oct 29 2020, 20:47:35 GMT

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45426
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/24/2020

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

RESULT:


Protocol	Port	Time
TCP	22	0:02:05

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 04/21/2019

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).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 443, 445.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

1-21,23-381,383-2868,2870-6128,6130-61999,64001-65535

SSH daemon information retrieving

port 22/tcp

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

Severity: 1

QID: 38047

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/03/2018

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentication methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentication methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

RESULT:

SSH1 supported	no
SSH2 supported	yes

Supported key exchange algorithms for SSH2	curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256
Supported host key algorithms for SSH2	ssh-ed25519
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password, keyboard-interactive


SSH Banner

port 22/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38050

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 10/29/2020

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:

The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

SSH-2.0-OpenSSH_8.2-hpn14v15 FreeBSD-openssh-portable-8.2.p1_1,1

Report Legend

Payment Card Industry (PCI) Status






The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.




A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels




A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.



Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.




Severity	Level	Description
 LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
 MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.




Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
	1	Minimal Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2	Medium Intruders may be able to determine the operating system running on the host, and view banner versions.
	3	Serious Intruders may be able to detect highly sensitive data, such as global system user lists.