COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	BPS Info Solutions, Inc.	ASV Company:	Comodo CA Limited
Date scan was completed:	07-05-2013	Scan expiration date:	10-03-2013

Part 2. Component Compliance Summary

IP Address : 64.74.121.2	Pass	Fail
IP Address : 74.116.32.10	Pass	Fail
IP Address : 74.116.32.11	Pass	Fail
IP Address : 74.116.32.20	Pass	Fail
IP Address : 74.116.32.21	Pass	Fail
IP Address : 74.116.32.22	Pass	Fail
IP Address : 74.116.32.23	Pass	Fail
IP Address : 74.116.32.24	Pass	Fail
IP Address : 74.116.32.25	Pass	Fail
IP Address : 74.116.32.26	Pass	Fail
IP Address : 74.116.32.27	Pass	Fail
IP Address : 74.116.32.28	Pass	Fail
IP Address : 74.116.33.1	Pass	Fail
IP Address : 74.116.34.1	Pass	Fail
IP Address : 74.116.35.1	Pass	Fail

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
64.74.121.2	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
64.74.121.2	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.74.121.2	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.74.121.2	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.74.121.2	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.74.121.2	Service Detection (GET request) ssl_client_tlsv1 (541/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.10	Postfix Cyrus SASL Authentication Context Data Reuse Memory Corruption (exploit) smtp (25/tcp) CVE-2011-1720	Medium	6.8	Pass	A newer fixed version of the software is used.
74.116.32.10	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Service Detection urd? (465/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Service Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.10	smtpscan SMTP Fingerprinting smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	SMTP Server Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	SMTP Authentication Methods smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Upgrade to Postfix 2.5.13 / 2.6.19 / 2.7.4 / 2.8.3 or later.

Disable this service if you do not use it, or filter incoming traffic to this port.
Review the list of methods and whether they're available over an encrypted channel.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.11	Postfix Cyrus SASL Authentication Context Data Reuse Memory Corruption (exploit) smtp (25/tcp) CVE-2011-1720	Medium	6.8	Pass	A newer fixed version of the software is used.
74.116.32.11	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Service Detection urd? (465/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Service Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.11	smtpscan SMTP Fingerprinting smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	SMTP Server Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	SMTP Authentication Methods smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Upgrade to Postfix 2.5.13 / 2.6.19 / 2.7.4 / 2.8.3 or later.

Disable this service if you do not use it, or filter incoming traffic to this port.
Review the list of methods and whether they're available over an encrypted channel.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.20	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.20	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.20	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

Reconfigure the affected application, if possible, to avoid use of RC4
ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.21	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.21	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.21	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.22	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.22	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.22	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.23	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.23	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.24	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.24	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Consolidated Solution/Correction Plan for above IP address:
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

Reconfigure the affected application, if possible, to avoid use of RC4
ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.25	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.25	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.25	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	CGI Generic Injectable Parameter www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Web Application Potentially Sensitive CGI Parameter Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	CGI Generic Tests Timeout www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.
Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.
Run your run scan again with a longer timeout or less ambitious options :

- Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'.

- Stop at first flaw = 'per port' is quicker.

- In 'some pairs' or 'some combinations' mode, try reducing web_app_tests.tested_values_for_each_parameter in nessusd.conf

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.26	FTP Supports Clear Text Authentication ftp (21/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.26	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	Service Detection ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	FTP Server Detection ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	FTP Service AUTH TLS Command Support ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS).
In the latter case, configure the server so that control connections
are encrypted.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.27	SSL Certificate Cannot Be Trusted https? (443/tcp)	Medium	6.4	Pass	The vulnerability is not present.
74.116.32.27	SSL RC4 Cipher Suites Supported https? (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.27	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL Certificate Information https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.27	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Open Port Re-check general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL Service Requests Client Certificate https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL / TLS Versions Supported https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL Cipher Suites Supported https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL Compression Methods Supported https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Purchase or generate a proper certificate for this service.
- Increase checks_read_timeout and/or reduce max_checks

- Disable any IPS during the Nessus scan

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.28	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.28	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.28	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server Directory Enumeration www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web mirroring www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Server Cookies Set www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.32.28	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server Directory Enumeration www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web mirroring www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Server Cookies Set www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	External URLs www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Consolidated Solution/Correction Plan for above IP address:
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

In order to ensure accurate results, change the web server's
configuration to allow access to Nessus.
Review the contents of the site's robots.txt file, use Robots META tags
instead of entries in the robots.txt file, and/or adjust the web
server's access controls to limit access to sensitive material.
Reconfigure the affected application, if possible, to avoid use of RC4
ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.33.1	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.33.1	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Inconsistent Hostname and IP Address general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.33.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Fix the reverse DNS or host file.
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

Reconfigure the affected application, if possible, to avoid use of RC4
ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.34.1	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.34.1	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Inconsistent Hostname and IP Address general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.34.1	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Fix the reverse DNS or host file.
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

Consolidated Solution/Correction Plan for above IP address:
Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.35.1	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.35.1	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Host Fully Qualified Domain Name (FQDN) Resolution general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Inconsistent Hostname and IP Address general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Nessus UDP scanner general/udp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	CGI Generic Tests Load Estimation (all tests) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
74.116.35.1	SSL Compression Methods Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	CGI Generic Tests Load Estimation (all tests) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Fix the reverse DNS or host file.
If you want to test them, re-scan using the special vhost syntax,
such as :

www.example.com[192.0.32.10]

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Part 3b. Special notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
74.116.32.28	Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	Directory Browsing: www (443/tcp)		

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
74.116.32.28	Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	Directory Browsing: www (80/tcp)		