

Part 1. Scan Information

Scan Customer Company:	BPS Info Solutions, Inc.	ASV Company:	Comodo CA Limited
Date scan was completed:	08/09/2014	Scan expiration date:	11/07/2014

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
------------	--------------------------------------	----------------	------------	-------------------	--

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 Sequence Prediction Blind Reset Spoofing DoS general/tcp CVE-2004-0230	Medium	5.0	Pass	Denial of service vulnerability
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
64.74.121.2	Nessus TCP scanner ssl_client_tlsv1 (541/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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.74.121.2	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Contact the vendor for a patch or mitigation advice.

Protect your target with an IP filter.

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	Service Detection urd? (465/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Nessus SYN scanner urd? (465/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
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	smtpscan SMTP Fingerprinting smtp (25/tcp)	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	Nessus SYN scanner smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	Patch Report 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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.10	TCP/IP Timestamps Supported general/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.

Protect your target with an IP filter.

Review the list of methods and whether they're available over an encrypted channel.

Disable this service if you do not use it, or filter incoming traffic to this port.

Install the patches listed below.

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	Service Detection urd? (465/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Nessus SYN scanner urd? (465/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
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	smtpscan SMTP Fingerprinting smtp (25/tcp)	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	Nessus SYN scanner smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	Patch Report 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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.11	TCP/IP Timestamps Supported general/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.

Protect your target with an IP filter.

Review the list of methods and whether they're available over an encrypted channel.

Disable this service if you do not use it, or filter incoming traffic to this port.

Install the patches listed below.

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	HTTP Cookie 'secure' Property Transport Mismatch www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HyperText Transfer Protocol (HTTP) Information 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	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Web Server Harvested Email Addresses 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	Web Server Directory Enumeration 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 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	SSL / TLS Versions Supported www (443/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
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	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	HTTP Server Cookies Set www (80/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	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.20	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	OS Identification 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	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

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	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
74.116.32.21	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Web Server robots.txt Information Disclosure 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	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Web Server Directory Enumeration 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	SSL Compression Methods Supported 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	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	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Anti-Nessus Defense Detection www (80/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	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.21	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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
74.116.32.21	Device Type 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	TCP/IP Timestamps Supported general/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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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.

Protect your target with an IP filter.

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
------------	--------------------------------------	----------------	------------	-------------------	--

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	SSL Session Resume Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server robots.txt Information Disclosure 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	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server Directory Enumeration 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	SSL Compression Methods Supported 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	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	Nessus TCP scanner 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
74.116.32.22	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.22	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	Device Type 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
74.116.32.22	TCP/IP Timestamps Supported general/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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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.

Protect your target with an IP filter.

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 Sequence Prediction Blind Reset Spoofing DoS general/tcp CVE-2004-0230	Medium	5.0	Pass	Denial of service vulnerability
74.116.32.23	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
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	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Anti-Nessus Defense Detection 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	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server Directory Enumeration 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	SSL / TLS Versions Supported 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	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
74.116.32.23	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.23	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	Device Type 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	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Contact the vendor for a patch or mitigation advice.

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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.

In order to ensure accurate results, change the web server's configuration to allow access to Nessus.

Consolidated Solution/Correction Plan for above IP address:

Protect your target with an IP filter.

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)	Low	2.6	Pass	
74.116.32.24	CVE-2013-2566				
74.116.32.24	HTTP Cookie 'secure' Property Transport Mismatch www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Web Server Harvested Email Addresses 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	Web Server Directory Enumeration 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 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	SSL / TLS Versions Supported 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

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	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	HTTP Server Cookies Set www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.24	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	OS Identification 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	TCP/IP Timestamps Supported general/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:

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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

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	TCP/IP Sequence Prediction Blind Reset Spoofing DoS general/tcp CVE-2004-0230	Medium	5.0	Pass	Denial of service vulnerability
74.116.32.25	SSL RC4 Cipher Suites Supported www (443/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.25	CGI Generic Tests HTTP Errors 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
74.116.32.25	HyperText Transfer Protocol (HTTP) Information 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 Server robots.txt Information Disclosure 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	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Anti-Nessus Defense Detection 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

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	HTTP Server Type and Version 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
74.116.32.25	Web Server Harvested Email Addresses 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	Web Server Directory Enumeration www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
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	SSL / TLS Versions Supported 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	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.25	Web Server Harvested Email Addresses www (80/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	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	Device Type 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	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Contact the vendor for a patch or mitigation advice.

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Consider increasing the 'maximum run time (min)' preference for the 'Web Application Tests Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- 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`

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.

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

In order to ensure accurate results, change the web server's configuration to allow access to Nessus.

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

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 Sequence Prediction Blind Reset Spoofing DoS general/tcp CVE-2004-0230	Medium	5.0	Pass	Denial of service 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
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
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	Service Detection ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	Nessus TCP scanner ftp (21/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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.26	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Contact the vendor for a patch or mitigation advice.

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.

Protect your target with an IP filter.

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 RC4 Cipher Suites Supported https? (443/tcp) CVE-2013-2566	Low	2.6	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL RC4 Cipher Suites Supported http? (80/tcp) CVE-2013-2566	Low	2.6	Pass	
74.116.32.27	SSL Cipher Suites Supported https? (443/tcp)	Low	0.0	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
74.116.32.27	SSL Compression Methods Supported 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	Service Detection https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Nessus SYN scanner https? (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL Cipher Suites Supported http? (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	SSL / TLS Versions Supported http? (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Service Detection http? (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	Nessus SYN scanner http? (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.27	TCP/IP Timestamps Supported general/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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

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	TCP/IP Sequence Prediction Blind Reset Spoofing DoS general/tcp CVE-2004-0230	Medium	5.0	Pass	Denial of service vulnerability
74.116.32.28	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
74.116.32.28	SSL Session Resume Supported 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	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	SSL Cipher Suites Supported 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	HTTP Server Type and Version 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	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	SSL Certificate Information 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
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	Nessus TCP scanner 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 (80/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	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	Anti-Nessus Defense Detection 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	HTTP Server Type and Version 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	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
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	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.32.28	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Contact the vendor for a patch or mitigation advice.

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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.

In order to ensure accurate results, change the web server's configuration to allow access to Nessus.

Protect your target with an IP filter.

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	HTTP Server Cookies Set www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Cookie 'secure' Property Transport Mismatch www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Web Server Harvested Email Addresses 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	Web Server Directory Enumeration 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 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	SSL / TLS Versions Supported www (443/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	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Server Cookies Set www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.33.1	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	OS Identification 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	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
74.116.33.1	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Fix the reverse DNS or host file.

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	Web Server Harvested Email Addresses www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HTTP Cookie 'secure' Property Transport Mismatch www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HTTP Methods Allowed (per directory) 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	Anti-Nessus Defense 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
74.116.34.1	HTTP Server Type and Version 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	Web Server Directory Enumeration 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 Certificate Information 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	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	Nessus SYN scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Web Server robots.txt Information Disclosure www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	HTTP Server Cookies Set www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Web Server Directory Enumeration www (80/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	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.34.1	Nessus SYN scanner www (80/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	Device Type 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	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
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	Inconsistent Hostname and IP Address general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

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.

In order to ensure accurate results, change the web server's configuration to allow access to Nessus.

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Fix the reverse DNS or host file.

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)	Low	2.6	Pass	
74.116.35.1	CVE-2013-2566 HTTP Cookie 'secure' Property Transport Mismatch 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	Anti-Nessus Defense Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HTTP Methods Allowed (per directory) www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Web Server robots.txt Information Disclosure www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HTTP Server Type and Version www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Web Server Harvested Email Addresses 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
74.116.35.1	Web Server Directory Enumeration 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 Compression Methods Supported 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	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	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Anti-Nessus Defense Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Web Server robots.txt Information Disclosure www (80/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	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	HTTP Server Cookies Set www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
74.116.35.1	Web Server Directory Enumeration www (80/tcp)	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	Nessus TCP scanner www (80/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	OS Identification 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	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

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. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Protect your target with an IP filter.

Fix the reverse DNS or host file.

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.33.1	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)		
74.116.33.1	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.20	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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.20	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.35.1	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)		
74.116.35.1	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.21	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)		
74.116.32.21	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.22	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)		
74.116.32.22	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.24	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)		
74.116.32.24	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.34.1	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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.34.1	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.23	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)		
74.116.32.23	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)		

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the

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	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
74.116.32.25	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)		
74.116.32.25	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)		