COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	rsync.net	ASV Company:	Comodo CA Limited
Date scan was completed:	06-02-2015	Scan expiration date:	08-31-2015

Part 2. Component Compliance Summary

IP Address : 69.43.165.11 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
69.43.165.11	OpenSSL 1.0.1 < 1.0.1j Multiple Vulnerabilities (POODLE) www (443/tcp) CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568	Medium	5.0	Pass	Denial of service vulnerability
69.43.165.11	OpenSSL 1.0.1 < 1.0.1j Multiple Vulnerabilities (POODLE) www (80/tcp) CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568	Medium	5.0	Pass	Denial of service vulnerability
69.43.165.11	SMTP Service Cleartext Login Permitted smtp (25/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Server CBC Mode Ciphers Enabled ssh (22/tcp) CVE-2008-5161	Low	2.6	Pass	
69.43.165.11	SSH Weak MAC Algorithms Enabled ssh (22/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
69.43.165.11	HyperText Transfer Protocol (HTTP) Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OpenSSL Version Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Server Type and Version 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
69.43.165.11	OpenSSL Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Perfect Forward Secrecy Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Certificate Information www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Cipher Block Chaining Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Cipher Suites Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL / TLS Versions Supported www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus TCP scanner www (443/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Web Server Harvested Email Addresses www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HyperText Transfer Protocol (HTTP) Information www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OpenSSL Version Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Methods Allowed (per directory) www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Server Type and Version www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Web Server Directory Enumeration www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection www (80/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus TCP scanner 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
69.43.165.11	DNS Server UDP Query Limitation dns (53/udp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Sender Policy Framework (SPF) Enabled dns (53/udp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Server Fingerprinting dns (53/udp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Server Detection dns (53/udp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Authentication Methods smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Service STARTTLS Command Support smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Server Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	smtpscan SMTP Fingerprinting smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus TCP scanner smtp (25/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Protocol Versions Supported ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Algorithms and Languages Supported ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Server Type and Version Information ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus TCP scanner ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Patch Report general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Device Type 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
69.43.165.11	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Additional DNS Hostnames general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	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 OpenSSL 1.0.1j or later.
Protect your target with an IP filter.
If you are sure that the DNS server will never return answers bigger than 512 bytes and that the client software prefers UDP (which is nearly certain), you may ignore this message.
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.
Configure the service to support less secure authentication mechanisms only over an encrypted channel.
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.
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
Install the patches listed below.
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

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
69.43.165.11	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Access: ssh (22/tcp)	The customer declares the software is implemented securely.	