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:	04-10-2017	Scan expiration date:	07-09-2017

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 < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32) 80 / tcp / www CVE-2016-2183	Medium	5.0	Pass	The vulnerability is patched
69.43.165.11	OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32) 443 / tcp / www CVE-2016-2183	Medium	5.0	Pass	The vulnerability is patched
69.43.165.11	SMTP Service Cleartext Login Permitted 25 / tcp / smtp	Low	2.6	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Server Detection 53 / udp / dns	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Service Detection 22 / tcp / ssh	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Server Fingerprinting 53 / udp / dns	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	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Web Server Harvested Email Addresses 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Server Detection 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Device Type 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	smtpscan SMTP Fingerprinting 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Service STARTTLS Command Support 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Algorithms and Languages Supported 22 / tcp / ssh	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Server Type and Version Information 22 / tcp / ssh	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Cipher Suites Supported 443 / tcp / www	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	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL Certificate Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Additional DNS Hostnames 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SMTP Authentication Methods 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OS Identification 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Patch Report 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSH Protocol Versions Supported 22 / tcp / ssh	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Sender Policy Framework (SPF) Enabled 53 / udp / dns	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OpenSSL Version Detection 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OpenSSL Version Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Server Type and Version 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP Server Type and Version 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	OpenSSL Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Web Application Sitemap 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	DNS Server UDP Query Limitation 53 / udp / dns	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	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	HTTP X-Frame-Options Response Header Usage 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus SYN scanner 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus SYN scanner 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus SYN scanner 25 / tcp / smtp	Low	0.0	Pass	The vulnerability is not included in the NVD
69.43.165.11	Nessus SYN scanner 22 / tcp / ssh	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Upgrade to OpenSSL version 1.1.0 or later, and ensure all 64-bit block ciphers are disabled. Note that upgrading to OpenSSL 1.1.0 does not completely mitigate this vulnerability; it simply disables the vulnerable 64-bit block ciphers by default.

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

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

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

www.example.com[192.0.32.10]

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

Install the patches listed below.

Configure the remote web server to use HSTS.

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.

Set a properly configured Content-Security-Policy header for all requested resources.

Set a properly configured X-Frame-Options header for all requested resources.

Protect your target with an IP filter.

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

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 o actions taken to either: 1)remov 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: 22 / tcp / ssh		