COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	rsync.net	ASV Company:	Sectigo Limited
Date scan was completed:	09-13-2019	Scan expiration date:	12-12-2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):216.66.77.198	Pass ☑	Fail □

Part 3a. Vulnerabilities Noted for each Component

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
216.66.77.198	No Credentials Provided 0 / tcp /	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	SSH Protocol Versions Supported 22 / tcp / ssh	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	SSH Algorithms and Languages Supported 22 / tcp / ssh	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	Nessus SYN scanner 22 / tcp / ssh	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	SSH Server Type and Version Information 22 / tcp / ssh	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	Service Detection 22 / tcp / ssh	Low	0.0	☑	□	The vulnerability is not included in the NVD
216.66.77.198	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	□	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Protect your target with an IP filter.

Part 3b. Special Notes by Component

Component	Special Note	Item Noted	Scan customer`s description of action taken and declaration that software is either implemented securely or removed
216.66.77.198	Remote Access	Remote Access: 22 / tcp / ssh	

Part 3c. Special notes -- Full Text

Note

Remote Access

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.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

IP_ADDRESS:216.66.77.198

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

216.66.77.198

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)

Requires description for each IP Address/range/subnet, domain, URL

82.197.184.218:

usw-s003.rsync.net: