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:	12-04-2018	Scan expiration date:	03-04-2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):64.62.236.78	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	
64.62.236.78	SSH Weak Algorithms Supported 22 / tcp / ssh	Medium	4.3	☑	☐	A compensating control is in place
64.62.236.78	SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam) 22 / tcp / ssh CVE-2015-4000	Medium	4.3	☑	☐	The software uses a secure configuration
64.62.236.78	FTP Supports Clear Text Authentication 21 / tcp / ftp	Low	2.6	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	SSH Server CBC Mode Ciphers Enabled 22 / tcp / ssh CVE-2008-5161	Low	2.6	☑	☐	
64.62.236.78	SSH Weak MAC Algorithms Enabled 22 / tcp / ssh	Low	2.6	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	FTP Server Detection 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	SSH Algorithms and Languages Supported 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	No Credentials Provided 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	Nessus SYN scanner 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	Nessus SYN scanner 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	Service Detection 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	Service Detection 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	SSH Server Type and Version Information 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.78	SSH Protocol Versions Supported 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Contact the vendor or consult product documentation to remove the weak ciphers.
Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
Protect your target with an IP filter.
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.
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.

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
64.62.236.78	Remote Access	Remote Access: 22 / tcp / ssh	
64.62.236.78	Insecure Services / industry-deprecated protocols	Insecure Services / industry-deprecated protocols: 21 / tcp / ftp	

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.

Insecure Services / industry-deprecated protocols

Note to scan customer: Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. 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:64.62.236.78

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

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

64.62.236.78

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: