COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Vines OS	ASV Company:	Sectigo Limited
Date scan was completed:	09-10-2019	Scan expiration date:	12-09-2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):52.203.207.79	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	
52.203.207.79	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Additional DNS Hostnames 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Service Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Service Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Service Detection 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Service Detection (2nd Pass) 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Service Detection (2nd Pass) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Nessus SYN scanner 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Nessus SYN scanner 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD

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	
52.203.207.79	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Application Sitemap 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Application Sitemap 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	OS Identification 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	TLS ALPN Supported Protocol Enumeration 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Device Type 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Apache HTTP Server Version 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Apache HTTP Server Version 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Server No 404 Error Code Check 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Server No 404 Error Code Check 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP Server Type and Version 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	HTTP Server Type and Version 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Server robots.txt Information Disclosure 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Server robots.txt Information Disclosure 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD

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	
52.203.207.79	SSL Certificate Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Site Cross-Domain Policy File Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
52.203.207.79	Web Site Cross-Domain Policy File Detection 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]
See below
Protect your target with an IP filter.
Configure the remote web server to use HSTS.
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.
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 that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.
Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

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

Part 3c. Special notes -- Full Text

Note

Part 4a. Scope Submitted by Scan Customer for Discovery

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

IP_ADDRESS:52.203.207.79

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

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

52.203.207.79

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

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