

Part 1. Scan Information

Scan Customer Company:	WineDirect	ASV Company:	Comodo CA Limited
Date scan was completed:	01/14/2019	Scan expiration date:	04/14/2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):siteadmin.uswest2.vin65.com	Pass <input checked="" type="checkbox"/>	Fail <input type="checkbox"/>
Component (IP Address, domain, etc.):www.winedirect.com	Pass <input checked="" type="checkbox"/>	Fail <input type="checkbox"/>

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	
siteadmin.uswest2.vin65.com	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Service Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Service Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Service Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Application Cookies Are Expired 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Application Cookies Are Expired 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Device Type 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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	
siteadmin.uswest2.vin65.com	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	OS Identification 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Apache HTTP Server Version 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Apache HTTP Server Version 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HTTP Server Type and Version 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	HTTP Server Type and Version 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Application Cookies Not Marked Secure 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Application Cookies Not Marked Secure 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Nessus SYN scanner 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Nessus SYN scanner 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Server robots.txt Information Disclosure 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	Web Server robots.txt Information Disclosure 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
siteadmin.uswest2.vin65.com	SSL Certificate Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

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

Consolidated Solution/Correction Plan for above IP address:

Configure the remote web server to use HSTS.

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Protect your target with an IP filter.

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.

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	
www.winedirect.com	Multiple Dangerous CGI Script Detection 443 / tcp / www CVE-2002-0749, CVE-2000-1023, CVE-2000-0977, CVE-2001-0420, CVE-2000-0952, CVE-2002-1526, CVE-2002-0263, CVE-2001-0562, CVE-2001-1196, CVE-2000-0526, CVE-2001-0023, CVE-1999-1072, CVE-2001-0100, CVE-2002-0203, CVE-2000-0288, CVE-2000-0923, CVE-2001-0123, CVE-2001-0022, CVE-2001-0180, CVE-2000-0423, CVE-2002-0955, CVE-2001-1212, CVE-2002-0346, CVE-2002-1334, CVE-2002-0917, CVE-1999-0937, CVE-1999-0934, CVE-1999-0935, CVE-2001-0099, CVE-2002-0750, CVE-2002-0611, CVE-2002-0751, CVE-2002-0752, CVE-2001-1343, CVE-2001-0076, CVE-2002-0710, CVE-2003-0153, CVE-2002-0230, CVE-2001-1205, CVE-2001-1283, CVE-2000-1131, CVE-2001-0135, CVE-2000-1132, CVE-1999-1374, CVE-2001-0133, CVE-2001-1100, CVE-1999-1377	High	10.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not present after inspection and testing
www.winedirect.com	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	SSL Certificate Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP Server Type and Version 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP Server Type and Version 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP X-Frame-Options Response Header Usage 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	TLS ALPN Supported Protocol Enumeration 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HyperText Transfer Protocol (HTTP) Redirect Information 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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	
www.winedirect.com	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	TLS NPN Supported Protocol Enumeration 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Device Type 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	nginx HTTP Server Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	nginx HTTP Server Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	JQuery Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Server robots.txt Information Disclosure 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Server No 404 Error Code Check 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	CGI Generic Injectable Parameter 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Nessus SYN scanner 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Nessus SYN scanner 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	CGI Generic Tests Load Estimation (all tests) 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Service Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Service Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Service Detection 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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	
www.winedirect.com	Web Application Cookies Not Marked HttpOnly 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Application Cookies Not Marked HttpOnly 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Application Sitemap 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Server Harvested Email Addresses 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Application Cookies Not Marked Secure 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	Web Application Cookies Not Marked Secure 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	OS Identification 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
www.winedirect.com	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:

Visit <http://cve.mitre.org/> and check the associated CVE entry for each script found. If you are running a vulnerable version, then delete or upgrade the script.

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

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

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

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.

Protect your target with an IP filter.

Configure the remote web server to use HSTS.

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

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.

DOMAIN:www.winedirect.com

DOMAIN:siteadmin.uswest2.vin65.com

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.

siteadmin.uswest2.vin65.com

www.winedirect.com

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)
Requires description for each IP Address/range/subnet, domain, URL

52.27.131.125:no connectivity to CDE

52.42.193.115:no connectivity to CDE

54.149.171.191:no connectivity to CDE

54.191.150.191:no connectivity to CDE

ec2-52-27-131-125.us-west-2.compute.amazonaws.com:no connectivity to CDE

ec2-52-42-193-115.us-west-2.compute.amazonaws.com:no connectivity to CDE

ec2-54-149-171-191.us-west-2.compute.amazonaws.com:no connectivity to CDE

ec2-54-191-150-191.us-west-2.compute.amazonaws.com:no connectivity to CDE

evineage.vin65.com:no connectivity to CDE

reports.vin65.com:no connectivity to CDE

siteadmin2.k1technology.com:no connectivity to CDE

winedirect.vin65.com:no connectivity to CDE

www.duckhorn.com:no connectivity to CDE

www.foleyfoodandwinesociety.com:no connectivity to CDE

www.twistedoak.com:no connectivity to CDE

www.vin65.com:no connectivity to CDE
