COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	IATAI ANDINA	ASV Company:	Comodo CA Limited
Date scan was completed:	08/06/2016	Scan expiration date:	06/09/2016

Part 2. Component Compliance Summary

IP Address : securews.allegraplatform.com 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
securews.allegraplatform.com	SSL Certificate Information 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Service Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Service Detection 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	CGI Generic Tests Load Estimation (all tests) 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	OS Identification 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HyperText Transfer Protocol (HTTP) Information 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
securews.allegraplatform.com	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Device Type 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Nessus SYN scanner 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Nessus SYN scanner 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Additional DNS Hostnames 0 / tcp /	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP Server Type and Version 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	HTTP Server Type and Version 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	SSL / TLS Versions 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
securews.allegraplatform.com	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD
securews.allegraplatform.com	OpenSSL Detection 443 / tcp / www	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Configure the remote web server to use HSTS.
Set a properly configured Content-Security-Policy header for all requested resources.
Protect your target with an IP filter.
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

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 of actions taken to either: 1)remove the software or 2) implement security controls to secure the