COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Beds24	ASV Company:	Comodo CA Limited
Date scan was completed:	11-28-2018	Scan expiration date:	02-26-2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):beds24.com	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	
beds24.com	SSL Anonymous Cipher Suites Supported 25 / tcp / smtp CVE-2007-1858	Low	2.6	☑	☐	
beds24.com	Network Time Protocol (NTP) Server Detection 123 / udp / ntp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	TLS ALPN Supported Protocol Enumeration 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Certificate Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Nessus SYN scanner 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Nessus SYN scanner 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Nessus SYN scanner 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP X-Frame-Options Response Header Usage 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	
beds24.com	HTTP X-Frame-Options Response Header Usage 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SMTP Service STARTTLS Command Support 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL / TLS Versions Supported 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Cipher Suites Supported 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Cipher Block Chaining Cipher Suites Supported 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Sitemap 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Sitemap 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Potentially Sensitive CGI Parameter Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection (2nd Pass) 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Service Detection (2nd Pass) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SMTP Server Detection 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Cookies Not Marked HttpOnly 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Cookies Not Marked HttpOnly 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP Server Type and Version 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP Server Type and Version 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Additional DNS Hostnames 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	smtpscan SMTP Fingerprinting 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	OS Identification 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	CGI Generic Tests Load Estimation (all tests) 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	
beds24.com	CGI Generic Tests Load Estimation (all tests) 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Cookies Not Marked Secure 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Application Cookies Not Marked Secure 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Apache HTTP Server Version 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Apache HTTP Server Version 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	ICMP Timestamp Request Remote Date Disclosure 0 / icmp / CVE-1999-0524	Low	0.0	☑	☐	
beds24.com	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	SSL Perfect Forward Secrecy Cipher Suites Supported 25 / tcp / smtp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Server Directory Enumeration 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	IP Protocols Scan 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	JQuery Detection 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	JQuery Detection 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	HTTP X-Content-Security-Policy Response Header Usage 80 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
beds24.com	Web Server Allows Password Auto-Completion 443 / tcp / www	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.
Set a properly configured X-Frame-Options header for all requested resources.
Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.
See below
Disable this service if you do not use it, or filter incoming traffic to this port.
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.
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]
Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.
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.

Configure the remote web server to use HSTS.
Reconfigure the affected application if possible to avoid use of weak ciphers.
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

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
beds24.com	Anonymous (non-authenticated) key-agreement protocols	Anonymous (non-authenticated) key-agreement protocols: 25 / tcp / smtp	

Part 3c. Special notes -- Full Text

Note

Anonymous (non-authenticated) key-agreement protocols

Note to scan customer: Due to increased risk of “man in the middle” attacks when anonymous (non-authenticated) key-agreement protocols are used, 1) justify the business need for this protocol or service to the ASV, or 2) confirm it is disabled/removed. 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.

DOMAIN:beds24.com

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

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

beds24.com

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

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

195.201.74.20:
new.beds24.com:
newadmin.beds24.com:
newapi.beds24.com: