Part 1. Scan Information

Scan Customer Company:	Direct Debit	ASV Company:	Comodo CA Limited
Date scan was completed:	02-14-2019	Scan expiration date:	05-15-2019

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):34.240.38.31 — 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	
34.240.38.31	Service Detection 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	HTTP X-Content-Security-Policy Response Header Usage 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	Device Type 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	HTTP X-Frame-Options Response Header Usage 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	OS Identification 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	Web Application Sitemap 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	HTTP Server Type and Version 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	Nessus SYN scanner 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	HTTP Methods Allowed (per directory) 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD
34.240.38.31	HyperText Transfer Protocol (HTTP) Information 8380 / tcp / www	Low	0.0	☑	☐	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.
Set a properly configured X-Frame-Options header for all requested resources.
Protect your target with an IP filter.

Part 3b. Special Notes by Component

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:34.240.38.31

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

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

34.240.38.31

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

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