



ASV Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Labor Law Poster Service	ASV Company:	McAfee
Date Scan Completed:	22-AUG-2012	Scan Expiration Date:	20-NOV-2012

Part 2. Component Compliance Summary

Device: 67.208.244.125 **Pass:** ☒ **Fail:** ☐

Part 3a. Vulnerabilities Noted for each IP Address

Device	Vulnerabilities Detected	Severity	CVSS	Status	Exceptions, False Positives, or Compensating Controls
67.208.244.125	Reverse NAT/Intercepting Proxy Detection Port: All Protocol: TCP URL: All	Low	3.6	Pass	Resolved By: Joey Sheets Reason: This is the desired use of these ip address. Ports go to different servers on the network running different OS's. This is a false positive. Approved By: McAfee Admin
67.208.244.125	HTTP Methods Allowed (per directory) Port: 443 Protocol: TCP URL: N/A	Low	2.6	Pass	None
67.208.244.125	TCP/IP Timestamps Supported Port: All Protocol: TCP URL: N/A	Low	2.6	Pass	None
67.208.244.125	Service Detection Port: 2280 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	SSH Protocol Versions Supported Port: 2280 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	SSH Server Type and Version Information Port: 2280 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	PPTP Detection Port: 1723 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	Service Detection Port: 443 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	Service Detection Port: 110 Protocol: TCP	Low	0.0	Pass	None

	URL: N/A				
67.208.244.125	Service Detection Port: 80 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	Default Apache Directories Detected Port: 80 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	DNS Server hostname.bind Map Hostname Disclosure Port: 53 Protocol: UDP URL: N/A	Low	0.0	Pass	None
67.208.244.125	DNS Server DNSSEC Aware Resolver Port: 53 Protocol: UDP URL: N/A	Low	0.0	Pass	None
67.208.244.125	DNS Server Detection Port: 53 Protocol: UDP URL: N/A	Low	0.0	Pass	None
67.208.244.125	DNS Server BIND version Directive Remote Version Disclosure Port: 53 Protocol: UDP URL: N/A	Low	0.0	Pass	None
67.208.244.125	Service Detection Port: 25 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	SMTP Server Detection Port: 25 Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	Web Application Scanner was unable to find Links/Forms Port: All Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	OS Identification Port: All Protocol: TCP URL: N/A	Low	0.0	Pass	None
67.208.244.125	ICMP Timestamp Request Remote Date Disclosure Port: All Protocol: ICMP URL: N/A	Low	0.0	Pass	None
	CVE-1999-0524				

**Consolidated
Solution/Correction
Plan for above IP
Address:**

All level medium and high vulnerabilities identified for this device must be addressed with mitigation or remediation in order to satisfy PCI requirements. Review all findings for this device, then for each vulnerability with level medium and high, implement the solution described or an equivalent solution. Regenerate and submit the report based on scan results taken after remediation is completed. If mitigations are employed according to the compensating controls mechanism of PCI, you must provide details of compensating controls for each level medium or high vulnerability that appears in this report.

Part 3b. Special Notes by IP Address

Device	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
67.208.244.125 Port: 1723 URL: N/A	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented	Remote Access Software	None	None

securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.		
---	--	--