



# PCI Security Report

Labor Law Poster Service

Report Generation Date: 22-AUG-2012 08:10

Scan Expiration Date: 20-NOV-2012 07:44

## Confidential Information

The following report contains confidential information. Do not distribute, email, fax or transfer via any electric mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone unless you confirm they are authorized to view the information.

## Disclaimer

This, or any other, vulnerability audit cannot and does not guarantee security. McAfee makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that McAfee shall be held harmless in any event. McAfee makes this information available solely under its Terms of Service Agreement published at [www.mcafeesecure.com](http://www.mcafeesecure.com).

## Disclosure

As a systems and networks security company, McAfee produces and sells a range of products separately from services provided as an Approved Scanning Vendor. McAfee security products include but may not be limited to the following categories: application or network firewalls, intrusion detection/prevention, database or other encryption solutions, security audit log solutions, anti-virus solutions

Table Of Contents	
Section	
1	Executive Summary
2	Certification of Regulatory Compliance
3.1	Device: 67.208.244.125
3.1.1	Overview
3.1.2	Open Ports
3.1.3	Consolidated Solution
3.1.4	Vulnerabilities
3.1.5	Resolved

## Executive Summary

McAfee has determined that 'Labor Law Poster Service' is **COMPLIANT** with the PCI scan validation requirement.

This report was generated by PCI Approved scanning vendor, McAfee, under certificate number 3709-01-06 in the framework of the PCI data security initiative.

As a Qualified Independent Scan Vendor McAfee is accredited by Visa, MasterCard, American Express, Discover Card and JCB to perform network security audits conforming to the Payment Card Industry (PCI) Data Security Standards.

To earn validation of PCI compliance, network devices being audited must pass tests that probe all of the known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e. viruses and worms) to gain access to or disrupt the network devices being tested.

**NOTE:** In order to demonstrate compliance with the PCI Data Security Standard a vulnerability scan must have been completed within the past 90 days with no vulnerabilities listed as severity ranking 3 or higher in the PCI management portal. In most cases, **MEDIUM** and **HIGH** rated vulnerabilities with the exception of specific denial of service (DOS) vulnerabilities must be remediated. Additionally, Visa and MasterCard regulations require that you configure your scanning to include all IP addresses, domain names, DNS servers, load balancers, firewalls or external routers used by, or assigned to, your company, and that you configure any IDS/IPS to not block access from the originating IP addresses of our scan servers.

## Certification of Regulatory Compliance

Sites are tested and certified daily to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC). They are also certified to meet the security scanning requirements of Visa USA's Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard International's Site Data Protection (SDP) program, American Express' CID security program, the Discover Card Information Security and Compliance (DISC) program within the framework of the Payment Card Industry (PCI) Data Security Standard.

### 3.1.1 - Overview: 67.208.244.125

Scan Date	Scan Expiration Date	Status
22-AUG-2012 07:44	20-NOV-2012 07:44	Pass

### 3.1.2 - Open Ports: 67.208.244.125

Port	Protocol	Service	Banner
25	tcp	smtp	smtp
53	tcp	domain	domain
53	udp	domain	domain
80	tcp	http	http
110	tcp	pop-3	pop3
443	tcp	https	https
1723	tcp	pptp	pptp
2280	tcp	Unknown	Invpoller

### 3.1.3 - Consolidated Solution: 67.208.244.125

All level 3, 4, and 5 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 3, 4, or 5, 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 3, 4, or 5 vulnerability that appears in this report.

### 3.1.4 - Vulnerabilities: 67.208.244.125

Severity	Name	Port	Category	Status
Low	Service Detection	2280/tcp	Other	Pass
<b>Description</b>  It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.				
<b>CVSS Score</b>  0.0				
<b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N				
<b>Solution</b>  n/a				
<b>Details</b>  :  An SSH server is running on this port.				
<b>Links</b>  None				
<b>References</b>  None				

Severity	Name	Port	Category	Status
Low	SSH Protocol Versions Supported	2280/tcp	Other	Pass
<b>Description</b>  This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>         The remote SSH daemon supports the following versions of the SSH protocol :  - 1.99 - 2.0  SSHv2 host key fingerprint : c3:42:fe:8b:12:59:25:76:0d:8d:f4:ac:44:20:f0:cf  <b>Links</b>  <a href="http://www.openssh.org">www.openssh.org</a> <a href="#">Modify SSH Config To Maximize Security</a> <a href="#">OpenSSH QuickRef (pdf)</a>  <b>References</b>  None				

Severity	Name	Port	Category	Status
Low	SSH Server Type and Version Information	2280/tcp	Other	Pass
<b>Description</b>  It is possible to obtain information about the remote SSH server by sending an empty authentication request.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>         :  <b>SSH version :</b> SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2 <b>SSH supported authentication :</b> publickey,password  <b>Links</b>				

[www.openssh.org](http://www.openssh.org)

#### References

None

Severity	Name	Port	Category	Status
Low	Remote Access Software Detected	1723/tcp	Other	Pass
Description				
Remote access software was detected on this network port.				
CVSS Score				
0.0				
CVSS Fingerprint				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
Solution				
MFE Recommendation / PCI Requirement				
<ul style="list-style-type: none"><li>• Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).</li><li>• Allow connections only from specific (known) IP/MAC addresses.</li><li>• Use strong authentication, including unique and complex passwords for logins according to PCI DSS Requirements 8.1 - 8.4 and 8.5.8-8.5.15.</li><li>• Enable encrypted data transmission according to PCI DSS Requirement 4.1.</li><li>• Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.</li><li>• Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.</li><li>• Restrict access to customer passwords to authorized reseller/integrator personnel.</li><li>• Enable the logging function.</li></ul>				
Details				
None				
Links				
None				
References				
None				

Severity	Name	Port	Category	Status
Low	PPTP Detection	1723/tcp	Windows	Pass
Description				
The remote host is running a PPTP (Point-to-Point Tunneling Protocol) server. It allows users to set up a tunnel between their host and the network the remote host is attached to.				
CVSS Score				
0.0				
CVSS Fingerprint				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
Solution				
Make sure use of this software is in agreement with your organization's security policy.				

## Details

It was possible to extract the following information from the remote PPTP server :

Firmware Version : 3790  
Vendor Name : Microsoft

## Links

None

## References

None

Severity	Name	Port	Category	Status
Low	HTTP Methods Allowed (per directory)	443/tcp	Web Server	Pass
<b>Description</b>  By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.  As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.  Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.  CVSS Score  2.6  CVSS Fingerprint  AV:N/AC:H/Au:N/C:P/I:N/A:N  Solution  This is informational, but knowing certain values of the Allow header field can help an attacker leveraged other attacks.				
<b>Details</b>  :  Based on the response to an OPTIONS request :  - HTTP methods GET HEAD OPTIONS POST are allowed on :  /  Based on tests of each method :  - HTTP methods GET HEAD OPTIONS POST are allowed on :  /  Links  <a href="#">OWASP</a>  References  None				

Severity	Name	Port	Category	Status
----------	------	------	----------	--------

<b>Low</b>	<b>Service Detection</b>	<b>443/tcp</b>	<b>Other</b>	<b>Pass</b>
<b>Description</b>  It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>  :  A web server is running on this port.  <b>Links</b>  None  <b>References</b>  None				

Severity	Name	Port	Category	Status
<b>Low</b>	<b>Service Detection</b>	<b>110/tcp</b>	<b>Other</b>	<b>Pass</b>
<b>Description</b>  It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>  :  A POP3 server is running on this port.  <b>Links</b>  None  <b>References</b>  None				

Severity	Name	Port	Category	Status
<b>Low</b>	<b>Service Detection</b>	<b>80/tcp</b>	<b>Other</b>	<b>Pass</b>

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

n/a

Details

:  
A web server is running on this port.

Links

None

References

None

Severity	Name	Port	Category	Status
Low	Default Apache Directories Detected	80/tcp	Other	Pass

Description

One or more of the following directories were found on the remote Apache webserver:

/\_borders/ /\_derived/ /\_fpclass/ /\_overlay/ /\_themes/ /\_themes/clean-curve/ /banners/ /banners// /banners//lavera/ /banners/q/ /banners/q/quote1 /banners/q/quote2 /banners/r/ /banners/r/real\_purity/ /banners/s/ /banners/s/sept04\_special/ /banners/s/sept04\_special2/ /fpdb/ /icons/ /icons/small/ /images/banners/

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

If you are not using the content in the default Apache directories, remove them as they may pose an information disclosure threat.

Details

Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_borders/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_derived/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_fpclass/						

Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_overlay/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_themes/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/_themes/clean-curve/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/banners/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/banners//						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/banners//lavera/						
Headers	Host=67.208.244.125						
Protocol	http	Port	80	Read Timeout	10000	Method	GET
Path	/banners/q/						
Headers	Host=67.208.244.125						

Links

[Apache Webserver Homepage](#)

References

None

Severity	Name	Port	Category	Status
Low	DNS Server hostname.bind Map Hostname Disclosure	53/udp	DNS	Pass
Description				
It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.				
CVSS Score				
0.0				
CVSS Fingerprint				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
Solution				
It may be possible to disable this feature. Consult the vendor's documentation for more information.				

#### Details

:

The remote host name is :

host.mydomainsatwork.com

#### Links

None

#### References

None

Severity	Name	Port	Category	Status
Low	DNS Server DNSSEC Aware Resolver	53/udp	DNS	Pass
<b>Description</b>  The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys.				
<b>CVSS Score</b>  0.0				
<b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N				
<b>Solution</b>  n/a				
<b>Details</b>  None				
<b>Links</b>  <a href="#">Information on DNSSEC Zone Leakage</a> <a href="#">Tool to Enumerate DNSSEC Zone Data</a> <a href="#">DNSSEC Homepage</a>				
<b>References</b>  None				

Severity	Name	Port	Category	Status
Low	DNS Server Detection	53/udp	Other	Pass
<b>Description</b>  The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.				
<b>CVSS Score</b>  0.0				
<b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N				
<b>Solution</b>  Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.				

## Details

### Synopsis :

A DNS server is listening on the remote host.

### Description :

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See also :

[http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)

### Solution :

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk factor :

None

### Links

[Wikipedia](#)

### References

None

Severity	Name	Port	Category	Status
Low	DNS Server BIND version Directive Remote Version Disclosure	53/udp	Bind	Pass
<b>Description</b>				
The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.				
This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.				
<b>CVSS Score</b>				
0.0				
<b>CVSS Fingerprint</b>				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
<b>Solution</b>				
It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf				
<b>Details</b>				
<b>Synopsis :</b>				
It is possible to obtain the version number of the remote DNS server.				
<b>Description :</b>				
The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.				
This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.				
<b>Solution :</b>				

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

Risk factor :

None

Plugin output :

The version of the remote DNS server is :

9.7.3

Other references : OSVDB:23

Links

None

References

Open Source Vulnerability Database 23

Severity	Name	Port	Category	Status
Low	DNS Server Detection	53/tcp	Other	Pass
<b>Description</b>				
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.				
<b>CVSS Score</b>				
0.0				
<b>CVSS Fingerprint</b>				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
<b>Solution</b>				
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.				
<b>Details</b>				
<b>Synopsis :</b>				
A DNS server is listening on the remote host.				
<b>Description :</b>				
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.				
<b>See also :</b>				
<a href="http://en.wikipedia.org/wiki/Domain_Name_System">http://en.wikipedia.org/wiki/Domain_Name_System</a>				
<b>Solution :</b>				
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.				
<b>Risk factor :</b>				
None				
<b>Links</b>				
<a href="#">Wikipedia</a>				
<b>References</b>				

Severity	Name	Port	Category	Status
Low	Service Detection	25/tcp	Other	Pass
<b>Description</b>  It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>  :  An SMTP server is running on this port.  <b>Links</b>  None  <b>References</b>  None				

Severity	Name	Port	Category	Status
Low	SMTP Server Detection	25/tcp	Mail Services	Pass
<b>Description</b>  The remote host is running a mail (SMTP) server on this port.  Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>  Disable this service if you do not use it, or filter incoming traffic to this port.  <b>Details</b>    <b>Synopsis :</b>  An SMTP server is listening on the remote port.  <b>Description :</b>  The remote host is running a mail (SMTP) server on this port.  Since SMTP servers are the targets of spammers, it is recommended you				

disable it if you do not use it.

Solution :

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk factor :

None

Plugin output :

Remote SMTP server banner :

220 host.mydomainsatwork.com ESMTP Postfix (Debian/GNU)

Links

[Sendmail](#)  
[Microsoft](#)

References

None

Severity	Name	Port	Category	Status
Low	Web Application Scanner was unable to find Links/Forms	All	Web Server	Pass
Description				
Web Application scan was incomplete/failed since Scanner did not find any Links or Forms to crawl on a open HTTP(s) port. This can be because of any of the following reasons:				
1. Open HTTP(s) port is not running WebServer or doesn't have any page(s).				
2. Only authorized user can access the pages.				
3. All the URL's on the root page are pointing to other websites.				
4. Pages/Resources are not linked on WebRoot/Index page.				
5. Login credential is required to access any pages/resources.				
6. This domain redirects to another domain (website).				
7. Scanner requests are blocked by network security products such as Web Application firewall, IPS etc.				
CVSS Score				
0.0				
CVSS Fingerprint				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
Solution				
Please ignore this message if reason 1, 2 or 3 is true.				
Reason 4: Please add Entry URLs. This option is available on Domain page --> Configure --> Scan Tab --> Entry URLs --> Add				
Reason 5: Run authenticated scans by adding username and password to scan configuration. (Please DO NOT USE "Administrator" or "Super User" Accounts!)				
Reason 6: If you own the domain this host is redirecting to, then ensure it's added for scanning.				
Reason 7: Ensure scans are not blocked by any network security product.				
For all other questions please contact McAfee SECURE Technical Support.				
Details				
No Links/Forms are found during the scan.				
Links				
None				
References				
None				

Severity	Name	Port	Category	Status
Low	TCP/IP Timestamps Supported	All	Other	Pass
<b>Description</b>  The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.  <b>CVSS Score</b>  2.6  <b>CVSS Fingerprint</b>  AV:N/AC:H/Au:N/C:P/I:N/A:N  <b>Solution</b>  n/a  <b>Details</b>          <b>Synopsis :</b>  The remote service implements TCP timestamps.  <b>Description :</b>  The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.  <b>See also :</b>  <a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a>  <b>Solution :</b>  n/a  <b>Risk factor :</b>  None  <b>Links</b>  <a href="http://www.ietf.org/rfc/rfc1323.txt">www.ietf.org/rfc/rfc1323.txt</a>  <b>References</b>  None				

Severity	Name	Port	Category	Status
Low	OS Identification	All	Other	Pass
<b>Description</b>  Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.  <b>CVSS Score</b>  0.0  <b>CVSS Fingerprint</b>  AV:N/AC:L/Au:N/C:N/I:N/A:N  <b>Solution</b>				

n/a

#### Details

#### Synopsis :

It is possible to guess the remote operating system.

#### Description :

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

#### Solution :

n/a

#### Risk factor :

None

#### Plugin output :

Remote operating system : Linux Kernel 2.6 on Debian 6.0 (squeeze)

Confidence Level : 75

Method : SSH

Not all fingerprints could give a match - please email the following to [os-signatures@McAfee.org](mailto:os-signatures@McAfee.org) :

HTTP:!:Server: Apache

SinFP:

P1:B11013:F0x12:W16384:O0204ffff:M1460:

P2:B11013:F0x12:W16384:O0204ffff010303000101080a00000000000000001010402:M1460:

P3:B00120:F0x04:W0:O0:M0

P4:4401\_7\_p=1723R

SMTP:!:220 host.mydomainsatwork.com ESMTP Postfix (Debian/GNU)

SSH:SSH-2.0-OpenSSH\_5.5p1 Debian-6+squeeze2

The remote host is running Linux Kernel 2.6 on Debian 6.0 (squeeze)

#### Links

None

#### References

None

Severity	Name	Port	Category	Status
Low	ICMP Timestamp Request Remote Date Disclosure	All	Other	Pass
Description				
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.				
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.				
CVSS Score				
0.0				
CVSS Fingerprint				
AV:N/AC:L/Au:N/C:N/I:N/A:N				
Solution				
Filter out the ICMP timestamp requests (13), and the outgoing ICMP				

timestamp replies (14).

#### Details

The remote clock is synchronized with the local clock.

CVE : CVE-1999-0524

Other references : OSVDB:94, CWE:200

#### Links

[BlackIce Block ICMP](#)

[BlackIce Admin Guide](#)

[National Vulnerability Database](#)

#### References

CVE CVE-1999-0524

Open Source Vulnerability Database 94

3.1.5 - Resolved: 67.208.244.125

Date	19-AUG-2012 22:59
Vulnerability	Reverse NAT/Intercepting Proxy Detection
Port	All
URL	All
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