ASV Scan Report Attestation of Scan Compliance

Scan Customer Information	Approved Scanning Vendor Information
Company: **David S. Marcus, Ph. D**	Company: **ComplyGuard Networks**
Contact:	Contact: **Support**
Tel: Title:	Tel: **(210) 835-2000** Title:
E-mail: **dsmarcus@earthlink.net**	E-mail: **support@complyguardnetworks.com**
Bus Address:	Bus Address: **412 North Main St.**
City: State/Province:	City: **San Antonio** State/Province: **TX**
Zip: URL:	Zip: **78205** URL: **www.complyguardnetworks.com**

Scan Status

- Compliance Status Fail ■ Pass □
- Number of unique components scanned: **1**
- Number of identified failing vulnerabilities: **6**
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- Date scan completed: **05/12/12**
- Scan expiration date (90 days from date scan completed): **08/10/12**

Scan Status

David S. Marcus, Ph. D attests on 05/12/12 that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. David S. Marcus, Ph. D also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

This scan and report was prepared and conducted by Complyguard Networks under certificate number 3710-01-03, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Complyguard Networks attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by support@complyguardnetworks.com.

ASV Scan Report Executive Summary

The Attestation of Scan Compliance is included as the cover sheet for this ASV Scan Report Executive Summary. Your bank, processor or ISO need only the Attestation of Compliance as your proof of compliance. This report is for your information and should be kept for your records. All High and Medium vulnerabilities MUST be remediated in order to obtain a PASS for the testing.

Part 1. Scan Information

Scan Customer Company: **David S. Marcus, Ph. D**	ASV Company: **ComplyGuard Networks**
Date scan was completed: **05/12/12**	Scan expiration date: **08/10/12**

Part 2. Component Compliance Summary

Fail ■

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS	Compliance	Exceptions, False Positives or Compensating Controls Noted by the ASV
	https (tcp/443) GET /LETtoaCuluFoy4DePCwPLiT0HI1s36zHz9s712uSci4zxnjnmPAmXpdcnGMYmVwDfBGtXI6zXgIJ1YC8lqJ0TYlUP8hajSNTWZJH7RUk1K6JHLGgGnDaMfSojaxweHvjcnRe3KKTJ8miLU3U3XnS4KZ4bihRqT2rIkowzQJHSk9VbbQ26pdrzLoImGB4v9lqUFyewXsahnz55dwjEDBNREZEbS7b67a<font%20size=50>DEFACED<!--//-- : MyWebServer 1.0.2 is vulnerable to HTML injection. Upgrade to a later version. CVE-2002-1453	Medium	4.3	Fail	

Consolidated Solution/Correction Plan for Above IP Address:

Currently, there are no known upgrades, patches, or workarounds available to correct this issue.

	https (tcp/443) GET /LETtoaCuluFoy4DePCwPLiT0HI1s36zHz9s712uSci4zxnjnmPAmXpdcnGMYmVwDfBGtXI6zXgIJ1YC8lqJ0TYlUP8hajSNTWZJH7RUk1K6JHLGgGnDaMfSojaxweHvjcnRe3KKTJ8miLU3U3XnS4KZ4bihRqT2rIkowzQJHSk9VbbQ26pdrzLoImGB4v9lqUFyewXsahnz55dwjEDBNREZEbS7b67a<font%20size=50>DEFACED<!--//-- : MyWebServer 1.0.2 is vulnerable to HTML injection. Upgrade to a later version. CVE-2002-1453	Medium	4.3	Fail	

Consolidated Solution/Correction Plan for Above IP Address:

Currently, there are no known upgrades, patches, or workarounds available to correct this issue.

<table>
<tr><th>IP Address</th><th>Vulnerabilities Noted per IP address</th><th>Severity Level</th><th>CVSS</th><th>Compliance</th><th>Exceptions, False Positives or Compensating Controls Noted by the ASV</th></tr>
<tr><td></td><td>http (tcp/80)
GET /LNSAZoL2iuV3PmcrZl0W5YhMwILOBPbZwzEHVi5QAMdlOJcFL6Y0Ihv21bU7R3461Q80T3CFq9WqFvx3lfcgsMIZ4MDac8YVcxkBralskmulwlrf5JnvLuewKZ402AkBLBIK0CZY7ajOn7U9xzZ0LAgwAzrUaw9UViczNtTyvEKhm7WnyF5dfR084QH966s324XgjXktxVXXaqe7xtf3d5bTukJXDoo<font%20size=50>DEFACED<!--//-- : MyWebServer 1.0.2 is vulnerable to HTML injection. Upgrade to a later version.
CVE-2002-1453</td><td>Medium</td><td>4.3</td><td>Fail</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
Currently, there are no known upgrades, patches, or workarounds available to correct this issue.</td></tr>
<tr><td></td><td>http (tcp/80)
GET /LNSAZoL2iuV3PmcrZl0W5YhMwILOBPbZwzEHVi5QAMdlOJcFL6Y0Ihv21bU7R3461Q80T3CFq9WqFvx3lfcgsMIZ4MDac8YVcxkBralskmulwlrf5JnvLuewKZ402AkBLBIK0CZY7ajOn7U9xzZ0LAgwAzrUaw9UViczNtTyvEKhm7WnyF5dfR084QH966s324XgjXktxVXXaqe7xtf3d5bTukJXDoo<font%20size=50>DEFACED<!--//-- : MyWebServer 1.0.2 is vulnerable to HTML injection. Upgrade to a later version.
CVE-2002-1453</td><td>Medium</td><td>4.3</td><td>Fail</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
Currently, there are no known upgrades, patches, or workarounds available to correct this issue.</td></tr>
<tr><td></td><td>https (tcp/443)
The remote Apache tomcat service is vulnerable to an information
CVE-2010-2227</td><td>Medium</td><td>6.4</td><td>Fail</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
Upgrade to version 5.5.30 / 6.0.28 or greater.</td></tr>
<tr><td></td><td>http (tcp/80)
The remote Apache tomcat service is vulnerable to an information
CVE-2010-2227</td><td>Medium</td><td>6.4</td><td>Fail</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
Upgrade to version 5.5.30 / 6.0.28 or greater.</td></tr>
</table>

<table>
<tr><th>IP Address</th><th>Vulnerabilities Noted per IP address</th><th>Severity Level</th><th>CVSS</th><th>Compliance</th><th>Exceptions, False Positives or Compensating Controls Noted by the ASV</th></tr>
<tr><td></td><td>x11 (tcp/6000)
Nmap has identified this service as Microsoft Terminal Service</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>isakmp (udp/500)
A VPN server is listening on the remote port.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
If this service is not needed, disable it or filter incoming trafficto this port.</td></tr>
<tr><td></td><td>https (tcp/443)
Nmap has identified this service as Apache Tomcat|Coyote JSP engine 1.1</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>https (tcp/443)
A web server is running on this port</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>https (tcp/443)
Links to external sites were gathered.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>https (tcp/443)
A web server is running on the remote host.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
</table>

<table>
<tr><th>IP Address</th><th>Vulnerabilities Noted per IP address</th><th>Severity Level</th><th>CVSS</th><th>Compliance</th><th>Exceptions, False Positives or Compensating Controls Noted by the ASV</th></tr>
<tr><td></td><td>https (tcp/443)
Some information about the remote HTTP configuration can be extracted.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>https (tcp/443)
This plugin determines which HTTP methods are allowed on various CGI</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>http (tcp/80)
Nmap has identified this service as Apache Tomcat|Coyote JSP engine 1.1</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>http (tcp/80)
A web server is running on this port</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>http (tcp/80)
Links to external sites were gathered.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>http (tcp/80)
A web server is running on the remote host.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
</table>

<table>
<tr><th>IP Address</th><th>Vulnerabilities Noted per IP address</th><th>Severity Level</th><th>CVSS</th><th>Compliance</th><th>Exceptions, False Positives or Compensating Controls Noted by the ASV</th></tr>
<tr><td></td><td>http (tcp/80)
Some information about the remote HTTP configuration can be extracted.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>http (tcp/80)
This plugin determines which HTTP methods are allowed on various CGI</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>general/udp (udp/0)
It was possible to obtain traceroute information.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>general/tcp (tcp/0)
The TCP initial sequence number of the remote host are incremented by random positive values.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>general/tcp (tcp/0)
It was possible to resolve the name of the remote host.</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
</table>

<table>
<tr><th>IP Address</th><th>Vulnerabilities Noted per IP address</th><th>Severity Level</th><th>CVSS</th><th>Compliance</th><th>Exceptions, False Positives or Compensating Controls Noted by the ASV</th></tr>
<tr><td></td><td>general/tcp (tcp/0)
The remote IP address seems to connect to different hosts</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
Make sure that this setup is authorized by your security policy</td></tr>
<tr><td></td><td>general/tcp (tcp/0)
Remote operating system : Microsoft Windows 2000</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
<tr><td></td><td>general/tcp (tcp/0)
It is possible to enumerate CPE names that matched on the remote</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b>
n/a</td></tr>
<tr><td></td><td>X11:3 (tcp/6003)
Nmap has identified this service as Microsoft Terminal Service</td><td>Low</td><td></td><td>Pass</td><td></td></tr>
<tr><td colspan="6"><b>Consolidated Solution/Correction Plan for Above IP Address:</b></td></tr>
</table>