COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	hajdhfkjahkdjf	ASV Company:	Comodo CA Limited
Date scan was completed:	02-19-2011 04:04	Scan expiration date:	05-20-2011 04:04

Part 2. Component Compliance Summary

IP Address : www.aqua.com	Pass	Fail
IP Address : 119.235.30.7	Pass	Fail

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.aqua.com	Multiple Vendor DNS Response Flooding Denial Of Service domain (53/udp) CVE-2004-0789	Medium	5.0	Pass	Denial of service vulnerability
www.aqua.com	SSL Certificate Expiry https (443/tcp)	Medium	5.0	Fail	
www.aqua.com	Web Server Uses Plain Text Authentication Forms http (80/tcp)	Medium	5.0	Fail	
www.aqua.com	Web Server Uses Basic Authentication http (80/tcp)	Low	2.6	Pass	
www.aqua.com	FTP Clear Text Authentication ftp (21/tcp)	Low	2.6	Pass	
www.aqua.com	Web mirroring https (443/tcp)	Low		Pass	
www.aqua.com	Web mirroring http (80/tcp)	Low		Pass	
www.aqua.com	HyperText Transfer Protocol Information https (443/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.aqua.com	HyperText Transfer Protocol Information http (80/tcp)	Low		Pass	
www.aqua.com	External URLs https (443/tcp)	Low		Pass	
www.aqua.com	External URLs http (80/tcp)	Low		Pass	
www.aqua.com	HTTP Cookies https (443/tcp)	Low		Pass	
www.aqua.com	Protected web pages https (443/tcp)	Low		Pass	
www.aqua.com	Protected web pages http (80/tcp)	Low		Pass	
www.aqua.com	HTTP Cookies http (80/tcp)	Low		Pass	
www.aqua.com	Web Server Allows Password Auto-Completion https (443/tcp)	Low		Pass	
www.aqua.com	Web Server Allows Password Auto-Completion http (80/tcp)	Low		Pass	
www.aqua.com	Web Server Uses Basic Authentication over HTTPS https (443/tcp)	Low		Pass	
www.aqua.com	smtpscan submission (587/tcp)	Low		Pass	
www.aqua.com	smtpscan smtp (25/tcp)	Low		Pass	
www.aqua.com	icmp timestamp request general/icmp CVE-1999-0524	Low		Pass	
www.aqua.com	TCP timestamps general/tcp	Low		Pass	
www.aqua.com	Common Platform Enumeration (CPE) general/tcp	Low		Pass	
www.aqua.com	FTP Server type and version ftp (21/tcp)	Low		Pass	
www.aqua.com	SMTP Server type and version submission (587/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.aqua.com	SMTP Server type and version smtp (25/tcp)	Low		Pass	
www.aqua.com	SSL Certificate Expiry - Future Expiry imaps (993/tcp)	Low		Pass	
www.aqua.com	SSL Certificate Expiry - Future Expiry pop3s (995/tcp)	Low		Pass	
www.aqua.com	Supported SSL Ciphers Suites imaps (993/tcp)	Low		Pass	
www.aqua.com	IMAP Banner imap (143/tcp)	Low		Pass	
www.aqua.com	IMAP Banner imaps (993/tcp)	Low		Pass	
www.aqua.com	DNS Server Detection domain (53/udp)	Low		Pass	
www.aqua.com	DNS Server on UDP and TCP domain (53/udp)	Low		Pass	
www.aqua.com	SPF Enabled domain (53/udp)	Low		Pass	
www.aqua.com	NTP read variables ntp (123/udp)	Low		Pass	
www.aqua.com	Host FQDN general/tcp	Low		Pass	
www.aqua.com	DNS Server Fingerprint domain (53/udp)	Low		Pass	
www.aqua.com	COMODO Invalid SSL Certificate https (443/tcp)	Low		Pass	
www.aqua.com	COMODO Invalid SSL Certificate pop3s (995/tcp)	Low		Pass	
www.aqua.com	COMODO Invalid SSL Certificate imaps (993/tcp)	Low		Pass	
www.aqua.com	HTTP Server type and version http (80/tcp)	Low		Pass	
www.aqua.com	HTTP Server type and version https (443/tcp)	Low		Pass	
www.aqua.com	OS Identification general/tcp	Low		Pass	
www.aqua.com	POP3 Server type and version pop3s (995/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.aqua.com	SSL ciphers https (443/tcp)	Low		Pass	
www.aqua.com	SSL ciphers pop3s (995/tcp)	Low		Pass	
www.aqua.com	SSL ciphers imaps (993/tcp)	Low		Pass	
www.aqua.com	SSH Server type and version ssh (22/tcp)	Low		Pass	
www.aqua.com	SSH protocol versions supported ssh (22/tcp)	Low		Pass	
www.aqua.com	POP3 Server type and version pop3 (110/tcp)	Low		Pass	
www.aqua.com	Services pop3s (995/tcp)	Low		Pass	
www.aqua.com	Services imap (143/tcp)	Low		Pass	
www.aqua.com	Services submission (587/tcp)	Low		Pass	
www.aqua.com	Services ssh (22/tcp)	Low		Pass	
www.aqua.com	Services https (443/tcp)	Low		Pass	
www.aqua.com	Services pop3 (110/tcp)	Low		Pass	
www.aqua.com	Services rsync (873/tcp)	Low		Pass	
www.aqua.com	Services http (80/tcp)	Low		Pass	
www.aqua.com	Services ftp (21/tcp)	Low		Pass	
www.aqua.com	OpenSSL Detection https (443/tcp)	Low		Pass	
www.aqua.com	OpenSSL Detection imaps (993/tcp)	Low		Pass	
www.aqua.com	OpenSSL Detection pop3s (995/tcp)	Low		Pass	
www.aqua.com	Services imaps (993/tcp)	Low		Pass	
www.aqua.com	Services smtp (25/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
www.aqua.com	Directory Scanner https (443/tcp)	Low		Pass	
www.aqua.com	IP protocols scan general/tcp	Low		Pass	
www.aqua.com	POP3 Service STLS Command Support pop3 (110/tcp)	Low		Pass	
www.aqua.com	Directory Scanner http (80/tcp)	Low		Pass	
www.aqua.com	IMAP Service STARTTLS Command Support imap (143/tcp)	Low		Pass	

Consolidated Solution/Correction Plan for above IP address:
Contact the vendor for an appropriate upgrade.
Purchase or generate a new SSL certificate to replace the existing one.
Make sure that every sensitive form transmits content over HTTPS.
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
Make sure that HTTP authentication is transmitted over HTTPS.
Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Disable this service if you do not use it, or filter incoming traffic to this port.
Purchase or generate a new SSL certificate in the near future to replace the existing one.
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.
If you are sure that the DNS server will never return answers bigger than 512 bytes and that the client software prefers UDP (which is nearly certain), you may ignore this message.
Ensure you have a SSL certificate issued by a legitimate CA
Install a valid SSL certificate
Disable this service if you do not use it.
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such that control connections are encrypted.

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
119.235.30.7	Multiple Vendor DNS Response Flooding Denial Of Service domain (53/udp) CVE-2004-0789	Medium	5.0	Pass	Denial of service vulnerability
119.235.30.7	SSL Certificate Expiry https (443/tcp)	Medium	5.0	Fail	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
119.235.30.7	Web Server Uses Plain Text Authentication Forms http (80/tcp)	Medium	5.0	Fail	
119.235.30.7	Web Server Uses Basic Authentication http (80/tcp)	Low	2.6	Pass	
119.235.30.7	FTP Clear Text Authentication ftp (21/tcp)	Low	2.6	Pass	
119.235.30.7	Web mirroring https (443/tcp)	Low		Pass	
119.235.30.7	HTTP Cookies https (443/tcp)	Low		Pass	
119.235.30.7	No 404 check http (80/tcp)	Low		Pass	
119.235.30.7	External URLs https (443/tcp)	Low		Pass	
119.235.30.7	External URLs http (80/tcp)	Low		Pass	
119.235.30.7	Protected web pages https (443/tcp)	Low		Pass	
119.235.30.7	Protected web pages http (80/tcp)	Low		Pass	
119.235.30.7	Web mirroring http (80/tcp)	Low		Pass	
119.235.30.7	HTTP Cookies http (80/tcp)	Low		Pass	
119.235.30.7	Web Server Allows Password Auto-Completion https (443/tcp)	Low		Pass	
119.235.30.7	Web Server Allows Password Auto-Completion http (80/tcp)	Low		Pass	
119.235.30.7	Web Server Uses Basic Authentication over HTTPS https (443/tcp)	Low		Pass	
119.235.30.7	smtpscan submission (587/tcp)	Low		Pass	
119.235.30.7	icmp timestamp request general/icmp CVE-1999-0524	Low		Pass	
119.235.30.7	TCP timestamps general/tcp	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
119.235.30.7	Common Platform Enumeration (CPE) general/tcp	Low		Pass	
119.235.30.7	FTP Server type and version ftp (21/tcp)	Low		Pass	
119.235.30.7	IMAP Banner imap (143/tcp)	Low		Pass	
119.235.30.7	SMTP Server type and version submission (587/tcp)	Low		Pass	
119.235.30.7	IMAP Banner imaps (993/tcp)	Low		Pass	
119.235.30.7	SMTP Server type and version smtp (25/tcp)	Low		Pass	
119.235.30.7	SSL Certificate Expiry - Future Expiry imaps (993/tcp)	Low		Pass	
119.235.30.7	SSL Certificate Expiry - Future Expiry pop3s (995/tcp)	Low		Pass	
119.235.30.7	DNS Server Detection domain (53/udp)	Low		Pass	
119.235.30.7	DNS Server Detection domain (53/tcp)	Low		Pass	
119.235.30.7	Supported SSL Ciphers Suites imaps (993/tcp)	Low		Pass	
119.235.30.7	NTP read variables ntp (123/udp)	Low		Pass	
119.235.30.7	DNS Server Fingerprint domain (53/udp)	Low		Pass	
119.235.30.7	Host FQDN general/tcp	Low		Pass	
119.235.30.7	Supported SSL Ciphers Suites pop3s (995/tcp)	Low		Pass	
119.235.30.7	COMODO Invalid SSL Certificate https (443/tcp)	Low		Pass	
119.235.30.7	COMODO Invalid SSL Certificate pop3s (995/tcp)	Low		Pass	
119.235.30.7	COMODO Invalid SSL Certificate imaps (993/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
119.235.30.7	HTTP Server type and version http (80/tcp)	Low		Pass	
119.235.30.7	HTTP Server type and version https (443/tcp)	Low		Pass	
119.235.30.7	OS Identification general/tcp	Low		Pass	
119.235.30.7	POP3 Server type and version pop3s (995/tcp)	Low		Pass	
119.235.30.7	SSL ciphers https (443/tcp)	Low		Pass	
119.235.30.7	SSL ciphers pop3s (995/tcp)	Low		Pass	
119.235.30.7	SSL ciphers imaps (993/tcp)	Low		Pass	
119.235.30.7	SSH Server type and version ssh (22/tcp)	Low		Pass	
119.235.30.7	SSH protocol versions supported ssh (22/tcp)	Low		Pass	
119.235.30.7	POP3 Server type and version pop3 (110/tcp)	Low		Pass	
119.235.30.7	Services imaps (993/tcp)	Low		Pass	
119.235.30.7	Services smtp (25/tcp)	Low		Pass	
119.235.30.7	Services imap (143/tcp)	Low		Pass	
119.235.30.7	Services pop3s (995/tcp)	Low		Pass	
119.235.30.7	Services https (443/tcp)	Low		Pass	
119.235.30.7	OpenSSL Detection pop3s (995/tcp)	Low		Pass	
119.235.30.7	Services rsync (873/tcp)	Low		Pass	
119.235.30.7	OpenSSL Detection imaps (993/tcp)	Low		Pass	
119.235.30.7	Services ssh (22/tcp)	Low		Pass	
119.235.30.7	Services http (80/tcp)	Low		Pass	

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
119.235.30.7	Services ftp (21/tcp)	Low		Pass	
119.235.30.7	Services submission (587/tcp)	Low		Pass	
119.235.30.7	Services pop3 (110/tcp)	Low		Pass	
119.235.30.7	OpenSSL Detection https (443/tcp)	Low		Pass	
119.235.30.7	IP protocols scan general/tcp	Low		Pass	
119.235.30.7	POP3 Service STLS Command Support pop3 (110/tcp)	Low		Pass	
119.235.30.7	Directory Scanner https (443/tcp)	Low		Pass	
119.235.30.7	IMAP Service STARTTLS Command Support imap (143/tcp)	Low		Pass	
119.235.30.7	Directory Scanner http (80/tcp)	Low		Pass	

Consolidated Solution/Correction Plan for above IP address:
Contact the vendor for an appropriate upgrade.
Purchase or generate a new SSL certificate to replace the existing one.
Make sure that every sensitive form transmits content over HTTPS.
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
Make sure that HTTP authentication is transmitted over HTTPS.
Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Disable this service if you do not use it, or filter incoming traffic to this port.
Purchase or generate a new SSL certificate in the near future to replace the existing one.
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.
Ensure you have a SSL certificate issued by a legitimate CA
Install a valid SSL certificate
Disable this service if you do not use it.
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such that control connections are encrypted.

Part 3b. Special notes by IP Address

IP Address	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