foundeo inc.
hackMyCF ColdFusion Security Scanner

Scan Results

Scan Date:
Tuesday November 8, 2016 at 16:13 UTC (less than one minute ago)
Server Name:
secure.qbillc.com

ColdFusion Server Security Report [secure.qbillc.com]

Operating System:	Windows 2012 R2
Web Server:	Microsoft-IIS/8.5

TLS / SSL Report

Common Name:	✓ *.qbillc.com
Certificate Expiration Date:	✓ May 31, 2017 (6 months)
Public Key Size:	✓ 2048 (2048 or greater recommended)
Signature Algorithm:	✓ sha256WithRSAEncryption
Certificate TrustStore Validation:	✓ Mozilla NSS 09/2016: ok ✓ Apple OS X 10.11.6: ok ✓ Microsoft 09/2016: ok ✓ Java 7 Update 79: ok ✓ Android 7.0.0 r1: ok
Contains Anchor Certificate:	✓ No
Valid Chain Order:	✓ Yes

Protocol Support:	✓ **SSLv2** Disabled (SSLv2 should be disabled, it has been considered weak for over 10 years and has been disabled in browsers by default since IE7) ! **SSLv3** Enabled Preferred Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (128 bit keysize) *HTTP 200 OK* (SSLv3 should be disabled, it has been considered weak since October 2014 due to the Poodle Vulnerability. Disabling may cause compatibility issues with IE on Windows XP, and old android clients) ! **TLSv1** Enabled Preferred Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (256 bit keysize) *HTTP 200 OK* (TLSv1 may be enabled for existing implementations, however PCI DSS 3.1 April 2015 § 2.2.3 states that: *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, ~~2016~~ 2018 (date changed) . Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS* Disabling TLS 1.0 may cause compatibility issues in Internet Explorer, see TLS Browser Support Chart.) ✓ **TLSv1.1** Enabled Preferred Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (256 bit keysize) *HTTP 200 OK* (TLS 1.1 may be considered an *early TLS* with respect to PCI DSS 3.1 compliance. Talk to your QSA for details.) ✓ **TLSv1.2** Enabled Preferred Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (256 bit keysize) *HTTP 200 OK* (TLS 1.2 should be enabled)
Compression Supported:	✓ No (Compression should be disabled due to CRIME)
Heartbleed:	✓ Not Vulnerable
Logjam:	✓ *No DHE Cipher Suites were accepted* (a unique 2028 bit DH group is recommended More Info)
Session Renegotiation:	✓ Client Initiated Session Renegotiation Disabled ✓ Secure Session Renegotiation Supported
OpenSSL CCS Injection	✓ Not Vulnerable More Info
Strict Transport Security	! Not Enabled More Info

We found **3 security issues** on your server secure.qbillc.com

important

SSL Version 3 Enabled

Your Web Server is accepting SSL V3 connections, vulnerabile

to the POODLE (CVE-2014-3566) attack. Consider disabling this protocol, which may impact old clients such as IE6 on Windows XP. Disabling SSLv3 may also impact server side HTTPS clients (that consume your web services or APIs), and potentially bots / crawlers. You can use our IIS SSL tool to disable SSLv3 on IIS: https://foundeo.com/products/iis-weak-ssl-ciphers/
More Information: https://poodle.io

warning

Server Header Version Disclosure
The HTTP Server header is disclosing version numbers. An attacker may use this to identify your server as vulnerabilities become known matching the version you are using.
More Information: http://www.petefreitag.com/item/419.cfm

warning

Server Software Disclosure
Your web server responds to each request with an unnecessary HTTP header *X-Powered-By* which contains information about software installed on the server. This information may be used to target your site as vulnerabilities become known.
More Information: http://www.petefreitag.com/item/722.cfm

Please note, this tool is not able to test for all potential security issues that may exist.

You're Not Using the Probe

A key feature of our paid accounts is the Probe, this is a file you download place on your server which gives HackMyCF more information it can use to find more vulnerabilities. [Learn More]()

Severity Key

Critical

Found 0 Critical Issues
These issues pose a significant security risk. It is imperative that they are resolved at once.

Important

Found 1 Important Issues
These issues may have a security risk in certain conditions. It is recommended that you resolve them.

Warning

Found 2 Warnings
You should consider fixing these issues, however, they do not pose a large risk.