Pressemitteilung

CAcerts Hauptsysteme durch Heartbleed-Bug nicht angreifbar

Die zentralen Systeme und die Stammzertifikate von CAcert sind von dem Fehler, der als „Heartbleed"-Bug bekannt geworden ist, **nicht** betroffen. CAcert kann deshalb mit Gewissheit sagen, dass die Zertifikate sicher unterschrieben worden sind und kein Schlüssel durch unsere Systeme kompromittiert worden ist.

Einige nicht-kritische Systeme, wie der Blog und das Wiki, haben jedoch die fehlerhaften Bibliotheken verwendet. Diese Systeme wurden noch am frühen Morgen auf den aktuellen Stand gebracht, so dass auch hier die sichere Kommunikation gewährleistet ist.

Um ein Maximum an Transparenz und Sicherheit auch für unsere Anwender zu gewährleisten, informieren wir zurzeit unsere Anwender von Server-Zertifikaten, dass sie gefährdet sind, wenn sie die fehlerhaften OpenSSL-Bibliotheken verwenden und wir erläutern, was zu tun ist.

121 Wörter, 885 Zeichen

1 Material zur Pressemitteilung

1.1 CAcert

Ziel von CAcert ist es kostenfreie Digitale Zertifikate nach dem X.509 Standard anzubieten. Diese Digitalen Zertifikate können zum Unterschreiben und Verschlüsseln von Dokumenten als auch zum Aufbau von gesicherten Datenverbindungen genutzt werden.

CAcert hat zur Zeit über 273.000 angemeldete Benutzer [1]

CAcert Inc. ein eingetragener Verein mit Sitz in New South Wales (NSW), Australia. CAcert Inc. hat ca. 100 Mitglieder und wurde am 24. Juli 2003 unter dem vollständigen Namen „CAcert Incorporated" mit der Incorporation Nummer INC9880170 gegründet. Die DUNS Nummer ist 75-605-6102. [2]

CAcert finanziert sich aus Spenden.

[1] https://www.cacert.org/stats.php
[2] https://wiki.cacert.org/CAcertInc

Mehr Informationen:
https://wiki.cacert.org/CAcertInShort-de
https://en.wikipedia.org/wiki/CAcert

2 Contact CAcert

Alexander Bahlo, Officer for Public Relations
pr@cacert.org