Press release

CAcert's main systems not vulnerable by OpenSSL heartbleed bug

The central systems of CAcert and its root certificates are **not** affected by the issue known as heartbleed bug. This means, our certificates are safe and no key was compromised by one of our systems.

For some non-critical systems, like the blog and the wiki, CAcert has fixed its servers after a few hours that the issue was published to assure a stable and secure communication.

To assure maximum transparency and security CAcert currently informs its users of server certificates that they might be affected when they have used the vulnerable OpenSSL library and we advise of what to do.

109 words 648 characters

1 Press release material

1.1 CAcert

The aim of CAcert is to offer free digital certificates that meet the X.509 standard. These digital certificates can be used to sign and encrypt documents as well as to establish secure data communication links.

The CAcert project has 273,000 registered users. [1]

CAcert Inc. is an incorporated non-profit association with approx. 100 members and is registered with New South Wales (NSW), Australia. - It was incorporated by 24 July 2003, with the full association name CAcert Incorporated under the Incorporation No INC9880170. Our DUNS number is 75-605-6102. [2]

CAcert is financed by donations.

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

More information about CAcert:
https://wiki.cacert.org/CAcertInShort-de
https://en.wikipedia.org/wiki/CAcert

2 Contact CAcert

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