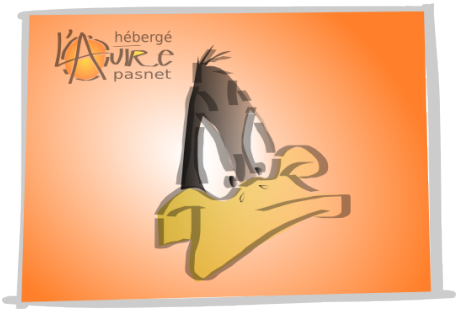
http://www.coincoin.fr.eu.org/?Disabling-SSL3-and-3DES-support-to



Disabling SSL3 and 3DES support to improve security for CAcert's users

- 6- Webographie -

Date de mise en ligne : lundi 20 octobre 2014

Copyright © L'Imp'Rock Scénette (by @_daffyduke_) - Tous droits réservés

CAcert intends to **disable SSL3 and 3DES** support for its main website www.cacert.org **by December 1, 2014**.

The main CAcert website is currently still supporting the SSL3 protocol for secure connections. However, in https://www.openssl.org/ bodo/ssl-poodle.pdf it is shown that SSL3 is susceptible to certain cryptograhical attacks. While www.cacert.org does support the recommended TLS_FALLBACK_SCSV option to protect clients with that same protocol option against unintended downgrades to SSL3, this still leaves plain old SSL3 clients vulnerable for the new attack.

Similarly, www.cacert.org is currently still supporting the 3DES cipher suite for encyrpting secure connections. However, this provides only 112 bits of security, which is below the currently recommended number of 128. Hence we should disable it to protect CAcert's clients.

In practice, the only client known to negotiate SSL3 with www.cacert.org is Internet Explorer 6.0 as found in Windows XP. Thus disabling SSL3 will block https access for these clients only. Similarly, 3DES will only be negotiated by IE 6 and IE 8 running on Windows XP. Since Windows XP is no longer supported by its vendor, and the widely circulated advice to all its users is to switch to a more recent operating system (or switch at least to a more current browser), announcing termination of support for SSL3 and 3DES by CAcert on December 1, 2014 does not seem unreasonable, and is fully in line with our mission to support the security of its users.

If you want to discuss this issue further, please use the bug tracker created for this issue (https://bugs.cacert.org/view.php?id=1314).

Copyright © L'Imp'Rock Scénette (by @_daffyduke_)