

## VeriSign bezpłatnie odnowi certyfikaty z kluczami wygenerowanymi pod Debianem

<http://ipsec.pl/kryptografia/2008/verisign-bezplatnie-odnowi-certyfikaty-z-kluczami-wygenerowanymi-pod-debianem>

{Firma VeriSign, właściciel marek GeoTrust, RapidSSL, thawte i VeriSign ogłasza dla wszystkich swoich Klientów program bezpłatnych odnowień certyfikatów SSL.

{  
Jednocześnie firma VeriSign informuje, iż główne certyfikaty (Root CA) używane do wystawiania certyfikatów SSL dostępnymi pod markami GeoTrust, RapidSSL, thawte i VeriSign są wolne od w/w luki.

{  
W związku z wykryciem krytycznej luki w bibliotece OpenSSL w systemach Debian, Ubuntu i pochodnych zalecane jest ponowne wygenerowanie kluczy i wystąpienie o odnowienie certyfikatów SSL. Odkryta luka w oprogramowaniu OpenSSL, pozwala na odgadnięcie kluczy szyfrujących, np. za pomocą metody brute-force. Problem dotyczy certyfikatów SSL wystawionych pomiędzy 17. września 2006 r., a 12. maja 2008 r.

{  
Jeżeli zachodzi podejrzenie, że klucz prywatny, który został użyty do wygenerowania pliku CSR (a tym samym certyfikatu SSL) był wygenerowany w w/w okresie za pomocą biblioteki OpenSSL w systemie Debian, Ubuntu lub pochodnym, zaleca się ponowne wygenerowanie klucza i wystąpienie o odnowienie certyfikatu.

{[ja href="http://www.gigaone.pl/certyfikaty-ssl/bezp](http://www.gigaone.pl/certyfikaty-ssl/bezp)