

Dziurawy OpenSSL w Debianie

<http://ipsec.pl/kryptografia/2008/dziurawy-openssl-w-debianie.html>

{W bibliotece OpenSSL w projekcie Debian GNU/Linux wykryto poważny błąd w implementacji generatora liczb losowych. W praktyce wszystkie wygenerowane za jej pomocą klucze kryptograficzne są przewidywalne i powinny być zainicjalizowane ponownie.

{Problem dotyczy dystrybucji Debian GNU/Linux oraz Ubuntu, ponieważ podatność została wprowadzona przez patch stosowany tylko w tych dystrybucjach. Pojawił się on w dystrybucji unstable 17 września 2006, a następnie stopniowo zostały przeniesione do testing i etch. Pakiety w dystrybucji sarge nie zawierają podatności. Podatność istnieje w debianowych wersjach pakietu openssl od 0.9.8c-1 do 0.9.8g-9. Brak podatności w swojej dystrybucji potwierdził m.in. Redhat.

{Administratorzy systemów opartych o Debiana powinni jak najszybciej zaktualizować system (np. przez apt-get update) oraz ponownie wygenerować klucze kryptograficzne dla wszystkich usług, dla których wygenerowano je za pomocą podatnych wersji OpenSSL.

{Wiecej informacji:

- <http://lists.debian.org/debian-security-announce/2008/msg00152.html>
- <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0166>
- <http://www.links.org/?p=327>