**CVE-2008-0166**

-Debian/Ubuntu System에서 OpenSSL library의 난수 생성과 관련한 취약점

-Debian OpenSSL 0.9.8c-4etch3 이전 버전 해당

-생성되는 난수가 예측 가능한 숫자인 것이 핵심

-따라서 Attacker가 암호화 키에 대해 brute force attack을 통해 이를 유추할 수 있음

해당 취약점과 관련한 Exploit-DB에 등록되어 있는 스크립트. Python, Perl, Ruby 총 세 가지의 언어로 작성되어 있다.

<https://www.exploit-db.com/search?cve=2008-0166>

또한 Exploit을 위한 암호화 키의 경우 아래 Github를 통해 다운로드 할 수 있다.

<https://github.com/g0tmi1k/debian-ssh>