

Debilidad criptográfica en los paquetes openssl de Debian.

There are no translations available

Luciano Bello, desarrollador argentino de Debian, ha descubierto que el generador de números aleatorios del paquete openssl de Debian es predecible, lo que implica una debilidad criptográfica bastante importante. Las claves afectadas incluyen las claves SSH, OpenVPN, DNSSEC, y las usadas en los certificados X.509 y en las sesiones SSL/TLS. Las claves generadas con GnuPG o GNUTLS no está afectadas.

La primera versión afectada por este problema es 0.9.8c-1 (sarge no está afectada). Para la distribución estable, estos problemas ya han sido corregidos en la versión 0.9.8c-4etch3. El proyecto Debian ha deshabilitado las conexiones con clave ssh como medida de seguridad en su infraestructura interna como respuesta. Elep enlaza en su bitácora con un programa que permite comprobar fácilmente si nuestras claves públicas OpenSSH o OpenVPN son lo suficientemente débiles como para que necesiten ser reemplazadas. Además indica cómo regenerar las claves RSA y DSA del servidor openssh-server, lo que es bastante recomendable.