'Severe' OpenSSL vuln busts public key crypto

By *srlinuxx*
Created *04/03/2010 - 10:12pm*
Submitted by srlinuxx on Thursday 4th of March 2010 10:12:05 PM Filed under Security [1]

Computer scientists say they've discovered a "severe vulnerability" in the world's most widely used software encryption package that allows them to retrieve a machine's secret cryptographic key.

The bug in the OpenSSL cryptographic library is significant because the open-source package is used to protect sensitive data in countless applications and operating systems throughout the world. Although the attack technique is difficult to carry out, it could eventually be applied to a wide variety of devices, particularly media players and smartphones with anti-copying mechanisms.

An OpenSSL official, who asked that his name not be published, said engineers are in the process of pushing out a patch and stressed the attack is difficult to carry out in real-world settings.

More details here [2]

Security

Source URL: http://www.tuxmachines.org/node/43632

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.theregister.co.uk/2010/03/04/severe_openssl_vulnerability/