

Link: <https://www.computerwoche.de/a/sicherheitsluecke-in-openssl-tls-server-erweiterung,2358141>

Patch verfügbar

Sicherheitslücke in OpenSSL TLS-Server-Erweiterung

Datum: 17.11.2010

Eine Schwachstelle in OpenSSL lässt sich unter Umständen zu DoS-Angriffen ausnutzen.

Ebenso anfällig sind Applikationen, die die entsprechenden Bibliotheken von OpenSSL verwenden. Auslöser ist eine Schwachstelle in der TLS-Erweiterung beim Verarbeiten von Code, durch die sich ein Buffer Overflow erzeugen lässt.

Ein erfolgreicher Angriff setzt voraus, dass der Server Multi-Threaded ist und die internen Caching-Mechanismen von OpenSSL verwendet. Die Sicherheitslücke ist für die Varianten 0.9.8f bis 0.9.8o, so wie 1.0.0 und 1.0.0a bestätigt. Die Entwickler **empfehlen**¹ das Verwenden der Versionen 0.9.8p, 1.0.0b oder das Einspielen der entsprechenden Patches. (TecChannel/wh)

Links im Artikel:

¹ http://www.openssl.org/news/secadv_20101116.txt
