PRESSEMITTEILUNG

"Heartbleed Bug": Informationssicherheit und Vertrauen bleiben Prioritäten für ein sicheres Internet

Berlin, 10.04.2014 - Informationssicherheit und Vertrauen in sichere Kommunikation müssen Priorität haben. Sichere Verschlüsselung ist essentiell für das Grundvertrauen im Internet. Die OpenSSL Lücke muss schnell geschlossen und SSL als Default gewählt werden.

Es ist bedauerlich, dass mit OpenSSL momentan eine Verschlüsselungssoftware Schlagzeilen macht, für die vorübergehend zu gelten scheint, dass auf sie zu verzichten sicherer sei, als sie zu nutzen. Bei OpenSSL handelt es sich um eine Open-Source-Implementierung des TLS-Protokolls. In OpenSSL wurde ein Fehler entdeckt, der als "Heartbleed Bug" bezeichnet wird. Durch diesen Fehler gibt eine OpenSSL-Instanz Daten preis, die normalerweise weder verschlüsselt noch unverschlüsselt sichtbar sind. TLS sieht eine Funktion namens "Heartbeat" vor. Mit dieser können sich Rechner gegenseitig Leernachrichten zuschicken, um damit anzuzeigen, dass alles in Ordnung ist. Mit einer entsprechend zusammengesetzten Nachricht kann ein Angreifer eine OpenSSL-Instanz dazu veranlassen, in einer vermeintlichen Leernachricht 64 KByte aus dem Hauptspeicher zu liefern. Darin kann eine E-Mail, ein Text oder sonst etwas enthalten sein – im schlechtesten Fall auch ein geheimer Schlüssel oder ein Passwort.

Klaus Schmeh (cv cryptovision GmbH), Kryptografie-Experte des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) kommentiert: "Das TLS-Protokoll selbst ist nicht fehlerhaft. Es wurde im Fall von OpenSSL nur falsch implementiert. Die Verschlüsselung, die das TLS-Protokoll durchführt, ist vom Heartbleed-Bug nicht betroffen (abgesehen davon, dass man damit an den Schlüssel herankommen könnte). Fehler wie den Heartbleed Bug hat es schon viele gegeben. Meist waren Programme betroffen, die nichts mit Kryptografie zu tun haben. Wenn ein Speicherzugriff nicht sauber programmiert ist, dann kann dies ein Einfallstor für Hacker sein. Der Heartbleed Bug war für die OpenSSL-Entwickler leicht zu korrigieren – ein paar zusätzliche Codezeilen genügten. Die korrigierte Version ist längst verfügbar."

Gerade vor dem Hintergrund des OpenSSL Bug gilt die Empfehlung von Sicherheitsexperten wie Bruce Schneier: "Je besser wir verschlüsseln, desto schwieriger wird es für diverse Schnüffler, uns zu überwachen - auch wenn nicht jede Verschlüsselung zu 100 Prozent sicher ist."

TeleTrusT – Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de