

[Sicherheit - Artikelübersicht](#), [Netz - Artikelübersicht](#), [Artikel zum tag: openssl](#), [Zertifikate - Artikelübersicht](#)

Hinweise zur "Heartbleed"-Sicherheitslücke in OpenSSL / Information des DFN-CERT

Mitte April 2014 ist unter dem Namen „Heartbleed“ eine schwerwiegende Sicherheitslücke in der Verschlüsselungsbibliothek OpenSSL bekannt geworden, über die sich auf betroffenen Systemen mit wenig Aufwand von außen sensible Informationen auslesen lassen. Da OpenSSL die mit Abstand am weitesten verbreitete Bibliothek zur Verschlüsselung von Daten darstellt und die verschiedensten Dienste wie Web oder Email darüber abgesichert werden, sind von dieser Schwachstelle zahlreiche große Systeme und Plattformen betroffen, die auch von Universitäten genutzt werden. Eine Zusammenstellung finden Sie unter anderem beim DFN:

<https://portal.cert.dfn.de/adv/DFN-CERT-2014-0420/>

Das Rechenzentrum hat alle zentral betriebenen Dienste inzwischen geprüft und die Systeme ggfs. aktualisiert. Da Angriffe über die Heartbleed-Lücke allerdings keinerlei Spuren auf den betroffenen Systemen hinterlassen, kann nicht ausgeschlossen werden, dass die Lücke zuvor bereits genutzt wurde, um Passwörter oder Zertifikatsdaten abzugreifen. Aus diesem Grund empfehlen wir allen Nutzern dringend, das Passwort ihres Uni-Accounts über <https://myaccount.uni-freiburg.de> zu ändern.

Alle Systemadministratoren der Universität, die nicht durch das RZ verwaltete Serversysteme betreiben, werden aufgefordert, diese zu überprüfen und gegebenenfalls die entsprechenden Security Advisories zu befolgen. Da sich über kompromittierte Zertifikate vertrauliche Daten auch im Nachhinein abgreifen lassen, wird zusätzlich dringend empfohlen, neben der Änderungen der Zugangsdaten zusätzlich die SSL-Zertifikate auszutauschen und die alten Zertifikate über die Universitäts-CA zurückziehen zu lassen. Eine Anleitung zur Erneuerung von Server-Zertifikaten finden Sie im RZ-Wiki: <https://wiki.uni-freiburg.de/rz/doku.php?id=opensslcert>

Weitere Informationen:

Über den Heartbleed-Test können Sie prüfen, ob Ihre Systeme betroffen sind:

<http://filippo.io/Heartbleed/>

Über folgenden Link erhalten Hinweise, welche Schritte für die Problemlösung erforderlich sind:

<http://heartbleed.com/>

Hintergrundinformationen zur Lücke finden Sie auf heise security:

<http://www.heise.de/security/meldung/Der-GAU-fuer-Verschluesselung-im-Web-Horror-Bug-in-OpenSSL-2165517.html>

<http://www.heise.de/newsticker/meldung/Passwort-Zugriff-Heartbleed-Luecke-mit-katastrophalen-Folgen-2166861.html>

From:

<https://wiki.uni-freiburg.de/rz/> - **RZ**

Permanent link:

<https://wiki.uni-freiburg.de/rz/doku.php?id=heartbleed>

Last update: **2014/04/23 11:25**

