Kritische Sicherheitslücken: TLS-Verschlüsselung für Java ließ sich auf mehreren Wegen knacken

Kritische Sicherheitslücken: TLS-Verschlüsselung für Java ließ sich auf mehreren Wegen knacken
Wie bei Heartbleed: TLS-Implementierung als Schwachstelle
In den vergangenen Tagen hat der Heartbleed-Angriff auf OpenSSL für Schlagzeilen gesorgt. Wie OpenSSL ist auch JSSE für Java eine TLS-Implementierung; Oracle stellt sie als Open Source-Software zur Verfügung. Über zwei der drei entdeckten Schwachstellen in JSSE konnten die IT-Sicherheitsforscher die Verschlüsselung mittels TLS komplett brechen. Sie informierten Oracle über die Sicherheitslücken, bevor sie diese öffentlich machten. Das Team um Prof. Dr. Jörg Schwenk rät, die Updates für Anwendungen, die JSSE nutzen, schnell zu installieren.
So lässt sich die TLS-Verschlüsselung in Java aushebeln
JSSE war anfällig für sogenannte Bleichenbacher-Angriffe. Die Forscher mussten einmal eine verschlüsselte Verbindung zwischen Server und Client - etwa einem Web-Browser - aufzeichnen. Anschließend stellten sie ein paar tausend Anfragen an den Server. Aus den Antworten des Servers konnten sie den Schlüssel berechnen und den aufgezeichneten Datenaustausch zwischen Server und Client entschlüsseln. Bei der ersten Schwachstelle gab der TLS-Server über Fehlermeldungen kritische Informationen weiter. Die zweite Schwachstelle basierte auf unterschiedlichen Antwortzeiten des JSSE-Servers. Bleichenbacher-Angriffe zählen zu den komplexesten kryptografischen Angriffen, den sogenannten adaptiven Chosen-Ciphertext-Angriffen.
April-Patch von Oracle löst weiteres Problem
Mit dem April-Patch fixt Oracle einen weiteren kryptografischen Algorithmus (PKCS#1 v2.1, auch bekannt als RSA-OAEP), der ebenfalls für einen adaptiven Chosen-Ciphertext-Angriff anfällig war, wie das Bochumer Team zeigte. Dieser Algorithmus steht nicht mit TLS in Zusammenhang, wird aber in anderen Anwendungen wie Web Services eingesetzt.
Weitere Informationen
Prof. Dr. Jörg Schwenk, Lehrstuhl für Netz- und Datensicherheit, Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität, 44780 Bochum, Tel. 0234/32-26692, E-Mail: joerg.schwenk@rub.de
Angeklickt
Blog-Post von RUB-Forscher Christopher Meyer zum "Oster-Hack"
 http://armoredbarista.blogspot.de/2014/04/easter-hack-even-more-critical-bugs-in.html
Informationen zu Heartbleed
 http://heartbleed.com/

Ruhr-Universität Bochum
Universitätsstraße 150
44780 Bochum
Deutschland
Telefon: 0234 32-201
Telefax: 0234 32-14201
URL: http://www.ruhr-uni-bochum.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=563176" width="1" height="1">

Pressekontakt

Ruhr-Universität Bochum

44780 Bochum

ruhr-uni-bochum.de

Firmenkontakt

Ruhr-Universität Bochum

44780 Bochum

ruhr-uni-bochum.de

Mitten in der dynamischen, gastfreundlichen Metropolregion Ruhrgebiet im Herzen Europas gelegen, ist die Ruhr-Universität mit ihren 20 Fakultäten Heimat von 5.000 Beschäftigten und über 36.500 Studierenden aus 130 Ländern. Alle großen wissenschaftlichen Disziplinen sind auf einem kompakten Campus vereint.Die Ruhr-Universität ist auf dem Weg, eine der führenden europäischen Hochschulen des 21. Jahrhunderts zu werden. Fast alle Studiengänge werden als Bachelor-Master-Programme angeboten. Unsere Exzellenzprogramme haben sich international einen Namen gemacht: Unsere Research School ist ein internationales Kolleg zur strukturierten Forschungspromotion in den Lebenswissenschaften, den Natur- und Ingenieurwissenschaften und den Geistes- und Gesellschaftswissenschaften. Untereinander, national und international stark vernetzte, fakultäts- und fachübergreifende Forscherverbünde (Research Departments) schärfen das Profil der RUB, hinzu kommen ein unübertroffenes Programm zur Förderung von Nachwuchswissenschaftlerinnen und -wissenschaftlern und eine hervorragende Infrastruktur.Lebendig wird all das durch die Menschen, die mit ihrem Wissensdurst, ihrer Neugier und ihrem Engagement auf dem Campus zusammentreffen und die Ruhr-Universität mitgestalten. Ihre Aufgeschlossenheit macht die RUB zum Anziehungspunkt für Menschen aus aller Welt. Die Wertetrias menschlich ? weltoffen ? leistungsstark ? gestalten den Lebensraum Ruhr-Universität. Dieser Raum umfasst mehr als nur die Summe seiner Einzelelemente: Menschlich-weltoffen heißt unterschiedliche Kulturen zu respektieren und Gästen Heimat zu geben. Menschlich-leistungsstark bedeutet gemeinsam schöpferische Kräfte zu entfalten und Neues mit Elan und Ehrgeiz anzupacken.Campus Ruhr-Universität ist die moderne universitas ? die Gemeinschaft, in der die Menschen im Zentrum stehen.