Heartbleed Zero-Day-Attacke: Welche Auswirkungen hat sie auf die Sicherheit?

Heartbleed Zero-Day-Attacke: Welche Auswirkungen hat sie auf die Sicherheit?

Kommentar von Lucas Zaichkowsky, Enterprise Defense Architect bei AccessData
Der 9. April 2014 hat das Potenzial, als bedeutungsvoller Tag in die Cybersecurity-Geschichtsbücher einzugehen. Während das Internet überschäumte mit Meldungen zur Einstellung des Supports von Microsofts Betriebssystem Windows XP, ist eine neue Schwachstelle aufgetaucht, die ich in Bezug auf mögliche Auswirkungen für eine der schwersten halte, die in letzter Zeit aufgetreten sind: die Heartbleed OpenSSL-Sicherheitslücke.
Kurz gesagt macht SSL-Verschlüsselung den Netzwerk- und Internet-Traffic unlesbar für jeden, der ihn abhören möchte, wodurch die übertragenen sensiblen Daten und persönliche Informationen geschützt werden. OpenSSL wird allgemein von Software verwendet, um SSL-Verschlüsselungen durchzuführen. Der Kern dieser Schwachstelle ist, dass Angreifer darüber die Verschlüsselungsschlüssel von Internet-Servern und Desktop-Software stehlen können, die OpenSSL zur Verschlüsselung des Netzwerk-Traffic einsetzen. Mit Hilfe dieser Schlüssel lassen sich Daten entschlüsseln. Was die Sache noch schlimmer macht: Selbst wenn die anfällige Software gepatcht wird, kann zuvor gespeicherte verschlüsselte Kommunikation mit den kompromittierten Schlüsseln dechiffriert werden.
Die Auswirkungen auf die Sicherheit sind damit sehr real - ein signifikanter Anteil der Software, die wir dieser Tage implementieren, nutzt die OpenSSL-Datenbank zur Verschlüsselung. Auf Grund dessen sind viele bekannte Server und Desktop-Software-Pakete betroffen, was wiederum Business-Server und -Desktops sowie Heimanwender Gefahren aussetzt.
Heartbleed ist ein hervorragendes Beispiel für Schwachstellen, die in Verschlüsselungslösungen lauern und nur darauf warten, entdeckt zu werden. Dieser spezifische Programmierungsfehler wurde mit OpenSSL-Version 1.0.1 im Dezember 2011 eingeführt. Kriminelle könnten ihn nutzen, Geheimdienste wie NSA könnten sich ihn zunutze machen - es ist schwer zu sagen, was genau diese Organisationen in ihrem "Arsenal" haben, denn es wird alles unter dem Deckmantel des Schweigens genutzt ?
Ich empfehle Unternehmen und Endnutzern, in den kommenden Wochen besonders streng darauf zu achten, dass ihre komplette Software gepatcht und auf dem aktuellsten Stand ist. Insbesondere für Systemadministratoren ist es unerlässlich, dass sie die Schwachstelle so schnell wie möglich stopfen. Am Markt gibt es dutzende kommerzielle Angebote, die beim Patch-Management unterstützen. Heimanwendern rate ich zur kostenfreien Secunia PSI-Software. Weitere Informationen und Tipps rund um die Heartbleed-Schwachstelle sind auf der Website des Forschungsteams unter http://heartbleed.com zu finden.
Über AccessData:
Die AccessData Group ist seit 25 Jahren Wegbereiter für Entwicklungen im Bereich der digitalen Ermittlungen und entsprechender Unterstützung in Rechtsstreitigkeiten. Die Produktfamilie besteht aus Stand-Alone- und Enterprise-Class-Lösungen mit dem Fokus auf Digital Forensik, E-Discovery und Cyber Security. Hierzu gehören unter anderem die Produkte FTK, SilentRunner, Summation und das CIRT Security Framework. Sie ermöglichen digitale Untersuchungen jeder Art, wie z.B. Computerforensik, Vorfallsanalyse, Hosted Review Services, rechtliche Nachprüfungen und Compliance-Audits. Mehr als 100.000 User, die weltweit im Gesetzesvollzug, in Regierungsbehörden, Unternehmen und Rechtanwaltskanzleien etc. tätig sind, vertrauen bereits auf die AccessData Software-Lösungen. AccessData ist zudem Anbieter für Trainings und Zertifizierungen in den Bereichen digitale Forensik und Rechtsstreitigkeiten. Weitere Informationen unter www.accessdata.com .

Weitere Informationen:
AccessData Group
Nicole Reid
International Marketing Manager
1 Bedford Street
3rd Floor
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
London
Ansprechpartner (in Deutschland):
Abdeslam Afras
Director, EMEA
 India
E-Mail: aafras@accessdata.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ms@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=563031" width="1" height="1">

Pressekontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Firmenkontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Weitere Informationen finden sich auf unserer Homepage