Whitepaper: POODLE SSLv3 Schwachstelle

SBA Research gGmbH

Version 1.0

presse@sba-research.org

15. Oktober 2014

Worum geht es?

Vor kurzem wurde eine neue Schwachstelle im SSL v3 Protokoll identifiziert[1]. Mittels dieser Schwachstelle ist es unter Umständen möglich, gewisse Teile einer verschlüsselten Verbindung auszulesen.

Was bedeutet das für mein Unternehmen?

In der Praxis können damit HTTP-Header wie zum Beispiel Session Cookies mitgelesen werden. Da für den Angriff jedoch eine Man-in-the-Middle Situation vorliegen muss, ist die Lücke nur eingeschränkt ausnutzbar. Zudem muss der Angreifer zumindest einen Teil des Klartextes kontrollieren was, ähnlich wie bei BEAST, beispielsweise durch Java Script bewerkstelligt werden kann. Das heißt, der Angreifer muss einen Teil der Infrastruktur für die Internetverbindung, (z.B. den WLAN Access Point) sowie bis zu einem gewissen Grad auch den Browser des Benutzers kontrollieren. Sie stellt bei weitem kein so großes Risiko wie beispielsweise die HEARTBLEED Lücke dar.

Version 3 des SSL Protokolls ist ein 1996 erstmals spezifiziertes Protokoll. Seit mehr als 10 Jahren gibt es mit TLS einen Nachfolger. Der Grund für die anhaltende Verwendung des SSL Protokolls liegt an der gewünschten Abwärtskompatibilität bei Clients und Servern. Aufgrund

[1] Poodle: https://www.openssl.org/~bodo/ssl-poodle.pdf

der häufigen Lücken im SSL Protokoll wie BEAST[2] im Jahr 2011, CRIME[3] im Jahr 2012 und jetzt POODLE birgt die Unterstützung dieser Legacy Protokolle ein zunehmend größeres Risiko.

Welche Gegenmaßnahmen kann ich treffen?

Um die Lücke gänzlich auszuschließen muss SSLv3 entweder am Client oder am Server deaktiviert werden. Dies hat zur Folge, dass keine SSLv3 Verbindungen mehr aufgebaut werden können.

Um das Risiko für die eigenen Systeme zu minimieren sollte mit der Deaktivierung von SSL 3.0 auf den Servern begonnen werden.

Da dies jedoch einige ältere Systeme wie zum Beispiel Windows XP mit dem Internet Explorer 6 aussperrt sollte dieser Schritt vorab geprüft werden. Aus den Logfiles der Webserver / Webapplikationen sollte ersichtlich sein ob bzw. wie viele dieser alten Systeme noch im Einsatz sind. Im Idealfall lässt sich daraus prozentuell ermitteln, wie viele Benutzer eine Deaktivierung von SSL 3.0 betreffen würde. Grundsätzlich wird jedoch wegen der fehlenden Unterstützung seitens Microsoft von einem Einsatz von Windows XP abgeraten.

Alle anderen Desktop Browser unterstützen zumindest TLSv1.0[4].

Bei mobilen Browsern (Android, iOS, Windows Phone, Blackberry) unterstützen alle aktuellen Geräte ebenfalls TLSv1.0. Auch ältere Versionen wie Android 2.3 und iOS 6 unterstützen zumindest TLS 1.0.

Bezüglich der Details zur Konfiguration von Servern (Apache, nginx, ISS; etc.) wird auf die sehr praxisorientierten Anleitungen von bettercrypto.org[5] verwiesen.

[2]BEAST: http://blog.ivanristic.com/2011/10/mitigating-the-beast-attack-on-tls.html

[3]CRIME: https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls

[4]https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0

[5]Bettercrypto.org Paper: https://bettercrypto.org/static/applied-crypto-hardening.pdf

Am Client lässt sich SSLv3 im Browser meist relativ einfach deaktivieren (IE [6], Firefox [7], Chrome [8]). Mozilla hat eine Extension veröffentlicht um SSLv3 in Firefox manuell zu deaktivieren, bis es in der nächsten Version am 25.11.2014 deaktiviert wird. Dies ist auch in gemanagten Netzwerken per Active Directory Group-Policy möglich. Die Konfigurationsanleitungen hierzu finden sich im entsprechenden Microsoft Advisory 3009008[9].

Bei mobilen Browsern ist es jedoch nicht möglich die Verwendung von SSL 3.0 explizit zu deaktivieren.

[6]Deaktivierung von SSLv3 im IE: https://technet.microsoft.com/library/security/3009008

[7]Deaktivierung von SSLv3 in Firefox 33: Unter `about:config` sollte `security.tls.version.min` auf `1` und `security.tls.version.max` auf `2` gesetzt werden

[8]Deaktivierung von SSLv3 in Chrome: Mittels Kommandozeilenparameter: `--ssl-version-min=tls1`

[9]MS Security Advisory: https://technet.microsoft.com/library/security/3009008