Fehler im WPA2-Protokoll ermöglichen Abhören von WLAN-Traffic

Sicherheitsforscher wollen noch heute Details zu mehreren Sicherheitslücken im Verschlüsslungsprotokoll WPA2 veröffentlichen. Sie lassen sich offenbar für eine Key Reinstallation Attack (KRACK) ausnutzen. Damit können Unbefugte den Datenverkehr zwischen Computern und WLAN-Routern oder WLAN-Access-Points entschlüsseln.

Dem Kryptographieexperten Kenn White zufolge handelt es sich um einen gravierenden Fehler auf Protokollebene. “Mögliche Folgen: WLAN-Entschlüsselung, Kapern von Verbindungen, Einschleusen von Inhalten”, deutet White auf Twitter an. Ihm zufolge sind die meisten oder möglicherweise sogar alle korrekten Implementierungen von WPA2 betroffen.

Update 17. Oktober 2017, 12 Uhr 22: *Inzwischen haben zahlreiche Experten zu der von der Lücke ausgehenden Gefahr Stellung genommen und mehrere Hersteller Patches zur Verfügung gestellt beziehungsweise angekündigt. Eine Übersicht finden Sie hier.*

Auch das US-CERT hat inzwischen vor KRACK gewarnt. Einem Bericht von Ars Technica zufolge basiert der Angriff auf mehren Fehlern beim Key Management im Vier-Wege-Handshake des Sicherheitsprotokolls WPA2. Das CERT/CC und die Forscher der belgischen Universität Leuven, von denen die Fehler gemeldet wurden, werden demnach Details dazu am 16. Oktober veröffentlichen.

Einer der Forscher sagte gegenüber Ars Technica, das Problem trete beim Aushandeln des Schlüssels für die Verschlüsselung des Datenverkehrs auf. Im dritten der insgesamt vier Schritte sei es möglich, den Schlüssel mehrfach zu senden. Wird das auf eine bestimmte Art getan, lasse sich ein Einmal-Schlüssel wiederverwenden. Das untergrabe die Verschlüsselung vollständig.

Alle Details wollen die Forscher erst am 1. November bei einem Vortrag auf der ACM Conference on Computer and Communications Security in Dallas verraten. Offenbar haben sie zudem die Website Krackattacks sowie eine GitHub-Seite reserviert. Dort sind dann weitere technische Details zu erwarten.

Wahrscheinlich sind Anbieter von WLAN-Produkten bereits informiert. Sie stellen möglicherweise bald Patches zur Verfügung. Allerdings erhalten vor allem für Verbraucher konzipierte WLAN-Router und WLAN-Access-Points von vielen Herstellern nur selten Updates. Darüber hinaus sind

dafür oft Eingriffe erforderlich, mit denen viele Verbraucher gar nicht vertraut sind.

[mit Material von Stefan Beiersmann, ZDNet.de]