WhatsApp gehackt, bitte Update einspielen

Facebook empfiehlt allen WhatsApp-Nutzern dringend, App und Betriebssystem auf den aktuellen Stand zu bringen. Betroffen sind sowohl Android als auch iOS.

(Bild: dpa, Martin Gerten)

WhatsApp leidet an einer Sicherheitslücke (CVE-2019-3568), die Unbefugten Fernzugriff auf das jeweilige Gerät erlaubt. Der Angreifer kann die Spyware einfach durch einen WhatsApp-Anruf in das jeweilige Gerät einschleusen, selbst wenn der Angerufene gar nicht abhebt. Seit Montagabend gibt es einen Patch.

WhatsApp-Betreiber Facebook ersucht alle User, ihre Applikation umgehend upzudaten. Auch das Betriebssystem, egal ob Android oder iOS, soll auf den aktuellen Stand gebracht werden.

Infos zur Schwachstelle

Die Lücke findet sich im VoIP-Stack von Whats App, **erläutert Facebook in einer Sicherheitswarnung**. Demzufolge könnte ein Angreifer präparierte SRTCP-Pakete an eine Zielrufnummer schicken und so einen Speicherfehler (buffer overflow) auslösen. Das endet in diesem Fall mit der Ausführung von Schadcode. Es ist davonauszugehen, dass die Sicherheitslücke als "**kritisch**" gilt.

Diese Whats-App-Versionen sind abgesichert - alle vorigen Ausgaben sind bedroht:

- Android: v2.19.134
- Business für Android: v2.19.44
- iOS: v2.19.51

- Business für iOS: v2.19.51
- Tizen: v2.18.15
- Windows Phone: v2.18.348

Anvisierter Menschenrechtsanwalt schlug Alarm

Laut *New York Times* steht die israelische Firma NSO unter Verdacht, die einschlägige Spyware programmiert zu haben. Der Fall ist demnach durch Angriffe auf einen Anwalt ins Rollen gekommen. Der Advokat bemerkte eine Reihe verpasster WhatsApp-Anrufe von angeblich skandinavischen Anschlüssen zu ungewöhnlichen Tageszeiten, woraufhin er sich an das Citizen Lab der Universität Toronto wandte.

Pikanterweise war der Anwalt an mehreren Klagen gegen NSO beteiligt. Darin wird der Firma vorgeworfen, Spyware vertrieben zu haben, die für Angriffe auf einen saudischen Dissidenten, einen Katari sowie mehrere mexikanische Journalisten genutzt wurde.

NSO gibt an, die eigenen Produkte nur an Regierungen zu lizenzieren und selbst keine Angriffsziele auszuwählen. Es soll ein firmeninternes Ethikkomitee geben, das anhand der Menschenrechtslage im jeweiligen Land entscheidet, ob NSO Spyware dorthin verkauft.

[UPDATE, 14.05.2019 08:50 Uhr] Angaben zu aktuellen WhatsApp-Versionen und Infos zur Lücke im Fließtext eingefügt.

Lesen Sie auch bei heise online:

- WhatsApp aktualisieren für Android - so geht's