

# **Warum die Stagefright-Sicherheitslücke für jeden Android-Nutzer gefährlich ist**

## **Warum die Stagefright-Sicherheitslücke für jeden Android-Nutzer gefährlich ist**

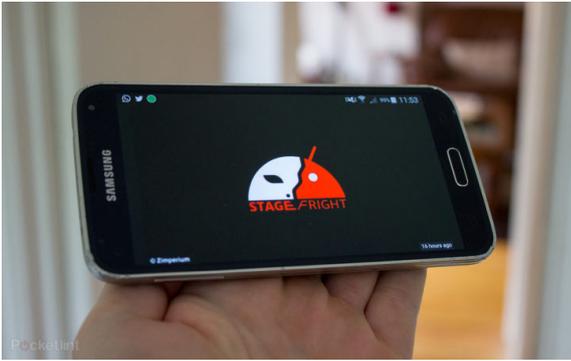
In Alarme & Ausbrüche, Sicherheitswissen by Jochen on October 5, 2015  
| Français, English, Deutsch

Eine Sicherheitslücke bei Android namens Stagefright wurde bei der Black Hat-Konferenz 2015 Anfang August publik gemacht. Wahrscheinlich haben Sie davon gehört, wie die Warnung durch die Medien ging, derzufolge Millionen Handys mit einer einzigen Nachricht gehackt werden könnten; doch stimmt das wirklich so? Falls ja, sollte Google (als Entwickler von Android) das Problem auf dem beliebten Betriebssystem doch sicherlich längst behoben haben, oder?

## **Was ist Stagefright und warum ist es so Besorgnis erregend?**

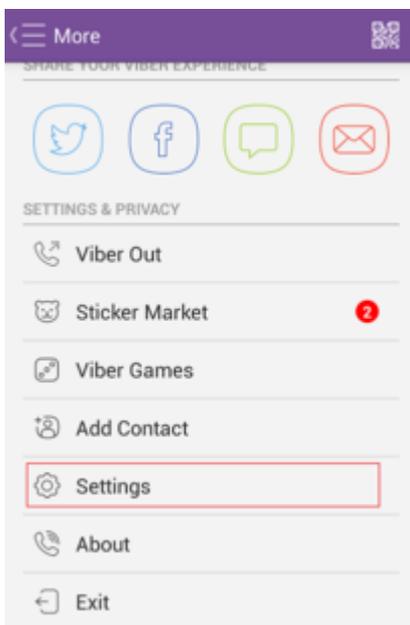
Heutzutage gehören regelmäßige Sicherheitslücken, Bugs und Warnmeldungen in technischen Belangen schon irgendwie dazu. Wieso sich auch verrückt machen, wenn es letzten Endes doch Sicherheitspatches dafür gibt, nicht wahr?

Leider ist die Sache bei der Stagefright-Sicherheitslücke nicht so einfach. Denken Sie an einen Katastrophenfilm, in dem ein riesiger Asteroid sich auf unheilvollem Kollisionskurs mit der Erde befindet und die Wissenschaftler trotz ihrer tollen Technologie keinen Weg finden, ihn auf eine andere Bahn zu lenken. Genauso verhält es sich im Prinzip mit Stagefright; denn auf Grund des Aufbaus des Android-Universums wird man sich in absehbarer Zeit nicht um das Problem kümmern und es ist lediglich eine Frage der Zeit, bis Stagefright auf zahllosen Geräten für katastrophale Folgen sorgt.

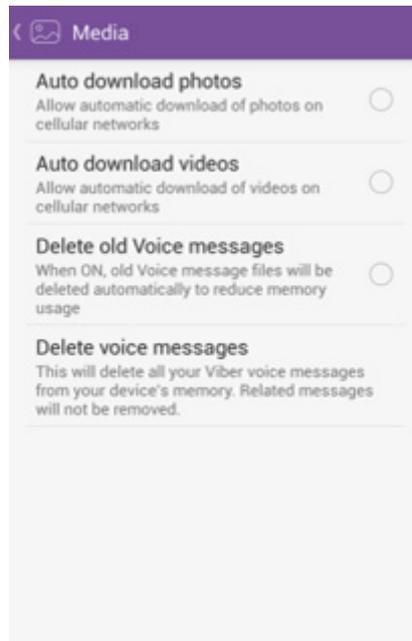
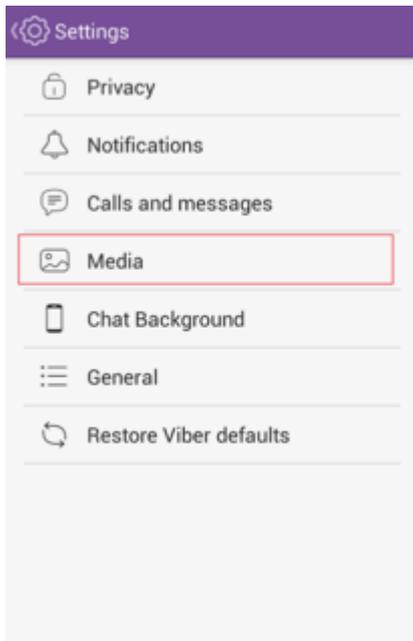


## Viber

Tippen Sie auf “Einstellungen” und dann “Medien”. Deaktivieren Sie die Option “Medium automatisch herunterladen”.

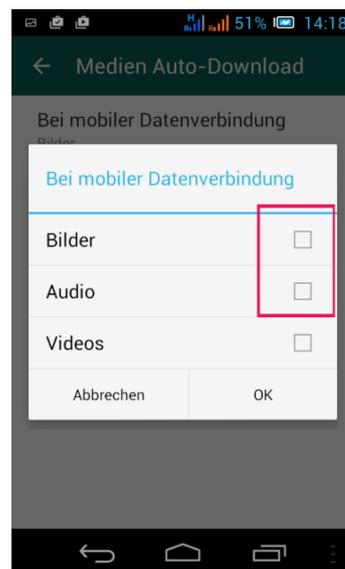
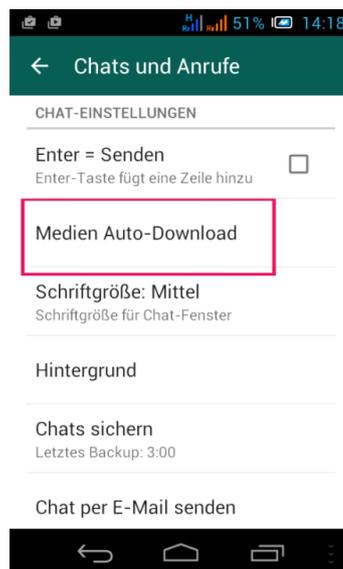
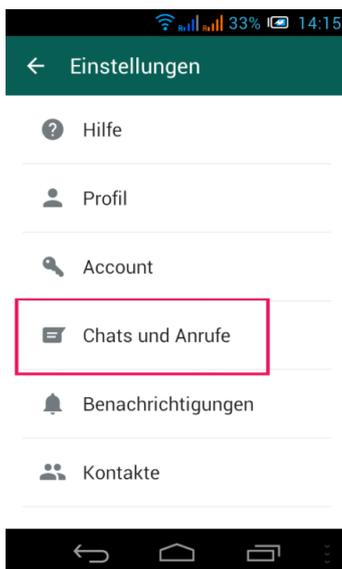


Quelle: ccm.net



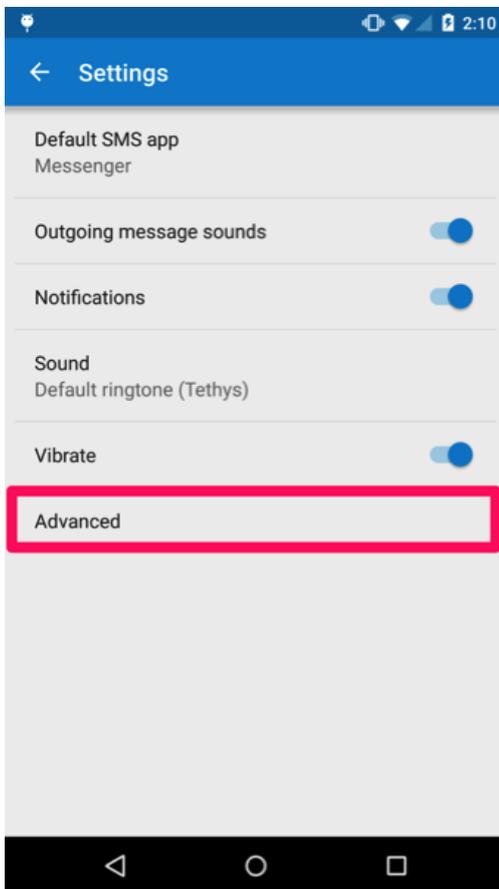
## WhatsApp

Wählen Sie "Einstellungen durch Tippen auf die drei Punkte und dann "Chats und Anrufe". Tippen Sie auf "Medien Auto-Download" und dann "Bei einer WLAN-Verbindung". Deaktivieren Sie die Option für Videos genauso wie unter "Bei mobiler Datenverbindung".

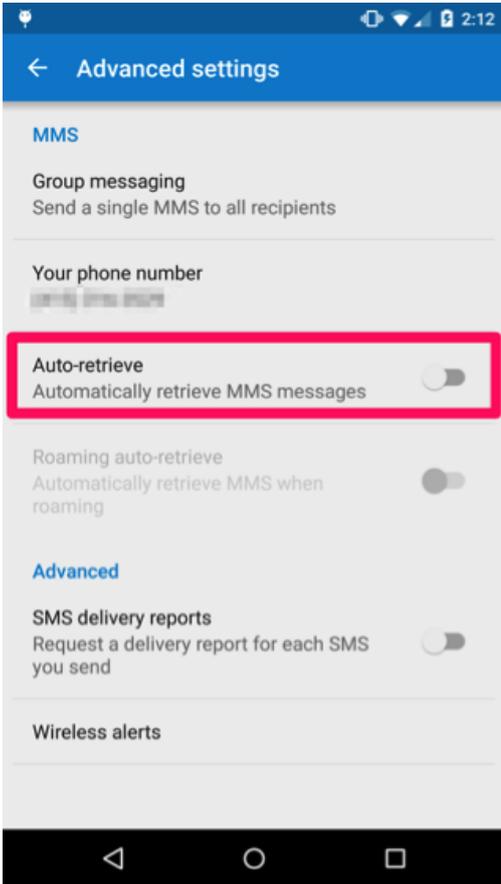


## Google Messenger

Tippen Sie auf die drei Punkte rechts oben. Wählen Sie “Einstellungen” und dann “Erweitert”. Deaktivieren Sie die Option “Automatisch abrufen”.



Quelle: Lookout



← Advanced settings

MMS

Group messaging  
Send a single MMS to all recipients

Your phone number

Auto-retrieve  
Automatically retrieve MMS messages

Roaming auto-retrieve  
Automatically retrieve MMS when roaming

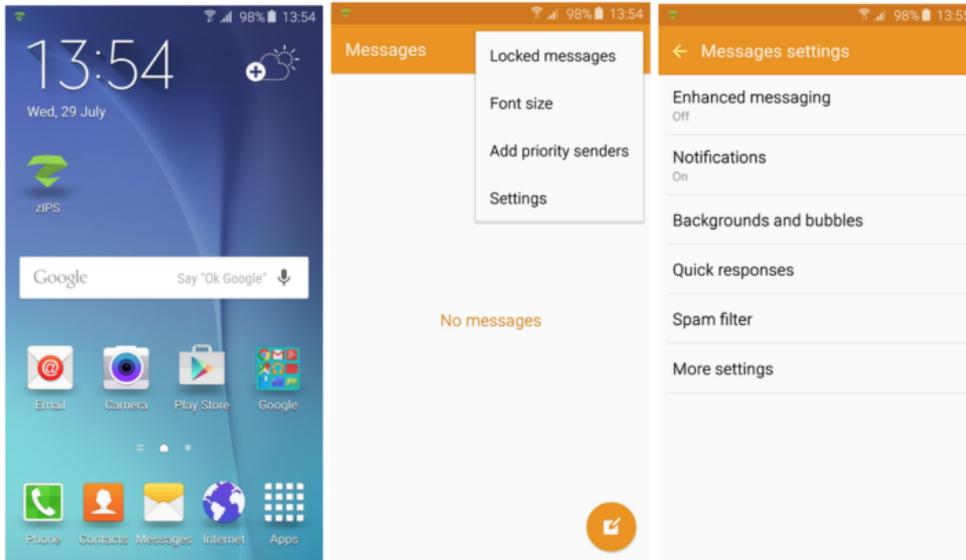
Advanced

SMS delivery reports  
Request a delivery report for each SMS you send

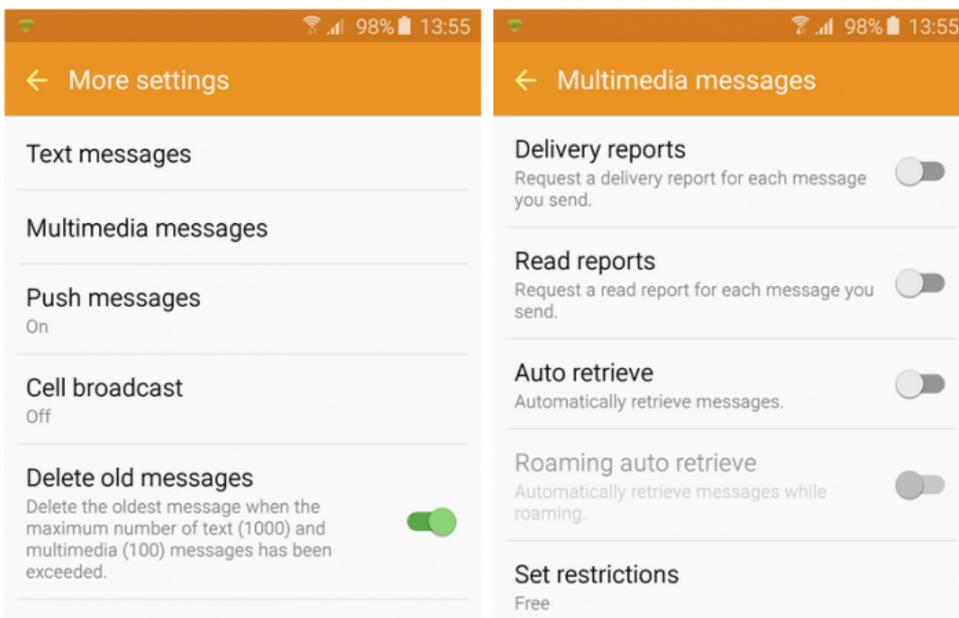
Wireless alerts

## Samsung Nachrichten

Gehen Sie zu "Mehr" und "Weitere Einstellungen". Deaktivieren Sie die Option "Automatisch abrufen".



Quelle: Zimperium



Quelle: Zimperium

Selbst nach Deaktivieren der Option zum automatischen Download sollten Sie Vorsicht walten lassen beim manuellen Laden von MMS aus unbekannter Quelle

und, um ganz sicher zu gehen, nicht einmal diejenigen von Freunden oder Ihrer Familie herunterladen. Diese können Sie unwissend in Gefahr bringen, wenn ihre Geräte betroffen sind.

## **Ihre Wahl als Verbraucher**

Während die meisten unter uns nicht über die Mittel verfügen, sich das neueste und tollste Modell jedes Geräts zu leisten, sollten Sie dennoch in Betracht ziehen, dass neuere Geräte in der Regel sicherer als aktuelle Modelle sind. Zusätzlich werden wichtige Sicherheitspatches und Updates üblicherweise nicht für Geräte bereitgestellt, die keine neueren Versionen von Android unterstützen.

Denken Sie daran: machen Sie sich mit den Betriebssystemen und Programmen vertraut, die Sie verwenden, und prüfen Sie regelmäßig auf neue Versionen. So war zum Beispiel auch Mozilla Firefox von der Stagefright-Sicherheitslücke betroffen, wobei das Problem allerdings seit Version 38 als behoben gilt.

## **Verschaffen Sie sich Gehör**

Die Mainstream-Medien mögen sich seit kurzem nicht mehr sonderlich für Stagefright interessieren, aber dessen ungeachtet sind immer noch Millionen von Menschen von diesem Bug betroffen. Bringen Sie Ihre eigenen Bedenken zum Ausdruck und bitten Sie Ihren Anbieter darum, Sie über das Problem auf dem Laufenden zu halten.

Wirbeln Sie in den sozialen Netzwerken Staub auf und markieren Sie Google, Ihren Anbieter und Ihren Hersteller in Ihren Posts. Leiten Sie Artikel zu Stagefright an die Menschen weiter, die Ihnen wichtig sind und Android genauso gern wie Sie nutzen.

## **Steigen Sie auf ein anderes Betriebssystem um**

Diese Option richtet sich eher an erfahrene Nutzer und ist den meisten Personen abzuraten. Dennoch ist es eine Alternative, die es häufiger zu erörtern gilt. Sollten Sie diese Option in Erwägung ziehen, raten wir Ihnen dazu, ein regelmäßig aktualisiertes ROM wie zu verwenden.

Dazu müssen Sie Ihr Gerät rooten, wodurch Sie allerdings Ihre Herstellergarantie verlieren können. Bitte bedenken Sie ebenso, dass Sie selbst dann nicht 100 %-ig

sicher vor Stagefright und anderen Sicherheitslücken sind. Der Vorteil ist: Sie haben weiterhin ein Android-Gerät, müssen jedoch nicht darauf warten, dass Hersteller und Anbieter Ihnen Patches bereitstellen, sondern erhalten diese umgehend.

Im Lauf der nächsten Monate können wir nur darauf hoffen, dass eine komplette Lösung für das Problem gefunden wird. Denken Sie daran: bleiben Sie zu Sicherheitsupdates auf dem Laufenden, abonnieren Sie entsprechende Newsletter und lesen Sie Blogs zur Sicherheit. Sprechen Sie mit Freunden und Familie darüber und treten Sie ein für Ihre Rechte an Ihrer Privatsphäre und Sicherheit als Verbraucher. Während die technische Entwicklung in beeindruckender Geschwindigkeit voranschreitet, nützen uns all diese tollen Geräte wenig, wenn wir uns in Richtung eines digitalen Armageddon bewegen. Denken Sie daran: Sicherheit ist ebenso wichtig wie Fortschritt.

Wir wünschen eine schöne (Sicherheitslücken-freie) Zeit!