Android-Lücken

In **Android Smartphones und Tablets** gibt es **schwere Sicherheitslücken**,
deswegen wende ich mich an Sie.

Für wen ist diese Information gedacht?
Wenn Sie ein Smartphone oder Tablet einsetzen, dass mit Android arbeitet,
sind Sie von den Sicherheitslücken betroffen.
Betroffen sind alle Android-Geräte seit Version 2.3 bis zur aktuellsten Version 5.1.1.

Wenn Sie ein Android Smartphone einsetzen, wenn in Ihrer Familie oder
im Freundeskreis jemand Android einsetzt, dann sollten auch Sie sich nach diesen
Informationen richten.

Lücke 1 – Stagefright

Android verwendet zum Anzeigen von Mediendateien eine SW-Komponente,
die unter dem Namen *Stagefright* bekannt ist. In dieser SW-Komponente steckt
ein schwerwiegender Fehler, der es erlaubt, über speziell präparierte Video-Dateien
Schadprogramme *(Malware)* in das System einzuschleusen.

Die Lücke ist so schwerwiegend, dass sich die Deutsche Telekom entschlossen hat,
die Zustellung von MMS *(Multimedia Messaging Services)* zu blockieren.
(Siehe: http://www.t-online.de/computer/sicherheit/id_74963432/android-luecke-stagefright-deutsche-telekom-blockt-mms.html)

Ob Ihr Gerät (noch) betroffen ist, können Sie mit einer speziellen App überprüfen,
die Sie über Google Play herunterladen können. Benutzen Sie dazu vorzugsweise die App
von der Firma, die die Lücke entdeckt hat.
(Download: https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector)

Lücke 2 – Certifi-Gate

In verschiedenen Apps zur Fernwartung, z.B. TeamViewer, RSupport und andere,
steckt eine Lücke, die es einer beliebigen Apps erlaubt, die volle Kontrolle zu übernehmen
und beispielsweise auch unbemerkt Audio-Aufnahmen zu machen und zu übertragen.
Das Smartphone wird somit zur Wanze.

Bekannt ist, dass auf manchen Premium-Smartphones von LG und Samsung die fehlerhafte
Komponente von RSupport vorinstalliert ist. Die Komponente ist als App nicht sichtbar
und kann auch nicht deinstalliert werden.

Auch hierfür gibt es eine App zum Testen von der Firma, die die Lücke entdeckt hat.
Nutzen Sie diese um zu überprüfen, ob Ihr Gerät betroffen ist.
(Download: https://play.google.com/store/apps/details?id=com.checkpoint.capsulescanner)

Mein Gerät ist betroffen – und nun?

Prüfen Sie über die Website des Herstellers Ihres Gerätes oder über die Website
Ihres Telefonanbieters, ob es Software-Updates für die jeweiligen Lücken gibt.
Ist dies nicht der Fall, müssen Sie Vorsichtsmaßnahmen ergreifen:

1 – Stagefright
Deaktivieren Sie alle Programme, die automatisch Videodateien entgegennehmen und anzeigen. Neben MMS gehören dazu WhatsApp, Google Hangout und FaceBook Messenger, aber auch das Anzeigen von Videos über den Browser oder von lokalen Speichermedien.
Soweit in den Anwendungen das automatische Anzeigen von Mediendateien unterdrückt werden kann (und Sie das so einstellen), können Sie die Anwendungen textbasiert verwenden.

Dass damit ein Smartphone seinen üblichen Einsatzzweck verliert, ist leider nicht zu ändern.

2 – Certifi-Gate
Betroffene Geräte sollten nicht mehr eingesetzt werden, bis ein Update vorliegt.
Da es unwahrscheinlich ist, dass für ältere betroffene Geräte noch Updates erscheinen, sollten diese Geräte sofort ersetzt werden.

Und andere Geräte?

Von den beschrieben Lücken sind ausschließlich Android Geräte betroffen. iPhones und Blackberry-Geräte sowie Geräte mit Windows Phone *(z.B. Lumia)* können weiterhin genutzt werden.