Steinbuch Centre for Computing

2020-05-25

Weitere Informationen und Anleitungen zur kritischen Sicherheitslücke in der Mail-App für iPhone und iPad (IOS-App „Mail“)

VERANLASSUNG
SCC-WARNUNG - vom 24.04.2020

BETREFF
Kritische Sicherheitslücke in der Mail-App für iPhone und iPad

HINWEIS
Aufgrund der Sicherheitslücke in der Mail-App für iPhone und iPad wurde am KIT für dienstlich bereitgestellte Geräte die Verwendung der App "Mail" vorübergehend untersagt und die Deinstallation empfohlen.

Apple stellt nun entsprechende Sicherheits-Updates zur Verfügung (iOS 13.5/12.4.7), welche die Sicherheitslücke beheben!

Nach der Aktualisierung der Geräte auf iOS 13.5 bzw. iOS 12.4.7 darf die App „Mail“ wieder genutzt werden.

Installation der Sicherheitsupdates

Das Update auf iOS 13.5 kann über OTA durchgeführt werden.
(Over the Air - in Einstellungen > Allgemein > Softwareupdate).

Stellen Sie sicher, dass ausreichend Akku-Kapazität und freier Speicherplatz vorhanden ist.
Eine vorherige Sicherung des Geräts ist zu empfehlen.

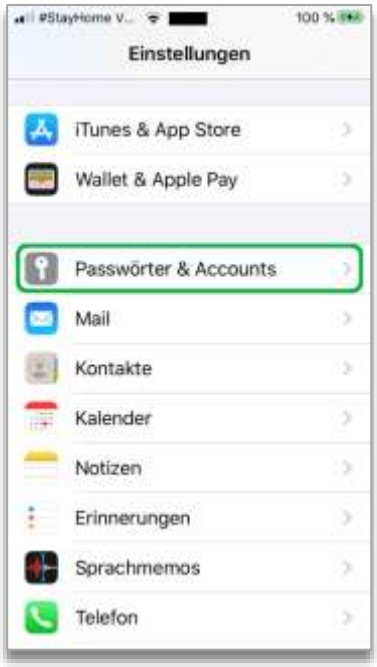
Bei manueller Installation laden Sie sich die Updates über https://developer.apple.com/news/releases/

2020-05-25

Re-Installation der Mail-App und Re-Synchronisation der Mails

1. Öffnen Sie Ihren Appstore und filtern Sie in der Suche nach „mail app“
2. Das **bekannte Mail Symbol** erscheint und wird mit einer **Wolke gekennzeichnet** – mit einem Klick darauf laden Sie die Mail-App herunter

3. Anschließend öffnen Sie unter **Einstellungen** den Bereich **Passwörter & Accounts**



4. Sie erhalten darunter eine Ansicht aller **Accounts**

5. Öffnen Sie den Account „**Exchange/KIT..“** und aktivieren Sie dort die Mails.

Beschreibung der Schwachstellen

Die iOS-App "Mail" ist auf allen iOS-Versionen rückwirkend bis iOS 6 von zwei schwerwiegenden Sicherheitslücken betroffen. Angreifern ist es dadurch möglich, durch das Senden einer E-Mail das betreffende iPhone oder iPad zu kompromittieren. Damit ist potentiell das Lesen, Verändern und Löschen von E-Mails möglich. Ob darüber hinaus weitere schädliche Aktivitäten für erfolgreiche Angreifer möglich sind, ist Gegenstand weiterer Prüfungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt diese Schwachstellen als sehr kritisch ein. Für die insgesamt zwei Schwachstellen stehen bislang keine Patches zur Verfügung. Medienberichten zufolge werden die Schwachstellen bereits aktiv ausgenutzt.
Anwender bekommen von der Attacke zunächst nichts mit, bis auf die Möglichkeit, dass die integrierte Mail-App eventuell langsamer läuft oder neu gestartet wird. Das aktive Öffnen der E-Mail in iOS 13 zur Ausführung des Angriffs ist somit nicht nötig. In iOS 12 müssen Anwender dagegen die bösartige Mail aktiv auswählen, dass der Angriff erfolgreich abläuft. Apple änderte mit iOS 13 die Funktionsweise der Mail-App; bereits beim Empfang einer Mail wird diese im Hintergrund heruntergeladen. Deshalb ist der Angriff bei iOS 13 auch ohne Nutzerinteraktion erfolgreich.

So lange keine entsprechenden Patches zur Verfügung stehen, sollten Anwender die App "Mail" unter Apple iOS deinstallieren (oder alternativ die mit dieser App verknüpften Accounts deaktivieren).

QUELLEN
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Warnung_iOS-Mail_230420.html

https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/

https://heise.de/-4710653
https://heise.de/-4726116

KONTAKT:
SCC Service Desk, Tel. -8000,
servicedesk@scc.kit.edu