2020-05-25

Further information and instructions on the critical security vulnerability in the mail app for iPhone and iPad (IOS app "Mail") …

____

CAUSE
SCC-WARNING – 24.4.2020

SUBJECT
Critical security vulnerability in mail app for iPhone and iPad

NOTE
Due to the security gap in the mail app for iPhone and iPad, KIT temporarily prohibited the use of the "Mail" app for devices provided for business purposes and recommended uninstalling it.

Apple now provides security updates (iOS 13.5/12.4.7) which fix the vulnerability!

After updating the devices to iOS 13.5 or iOS 12.4.7 the app "Mail" may be used again.

Installation of security updates

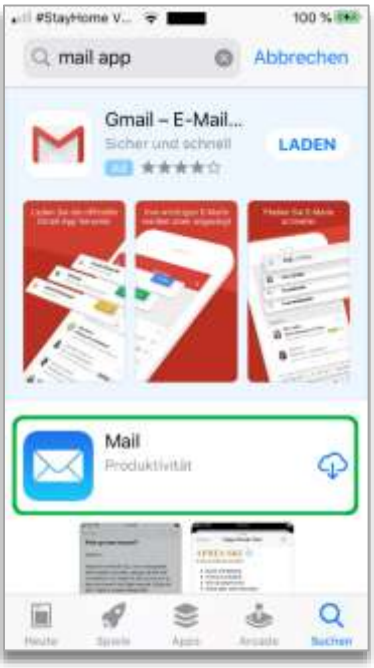
The update to iOS 13.5 can be performed via OTA.
(Over the Air - in Settings > General > Software Update).

Make sure that there is sufficient battery capacity and free memory.
It is recommended to back up the device beforehand.

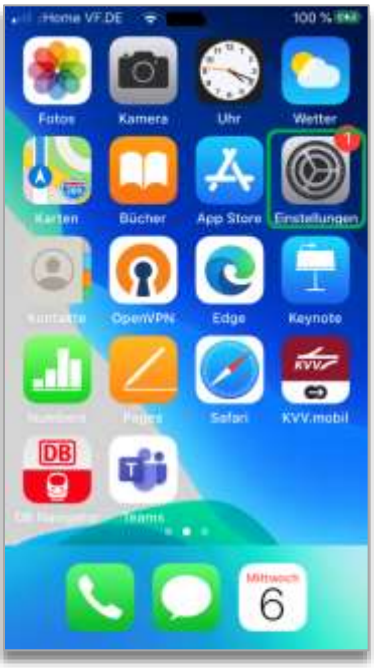
In case of manual installation, please download the updates from
https://developer.apple.com/news/releases/

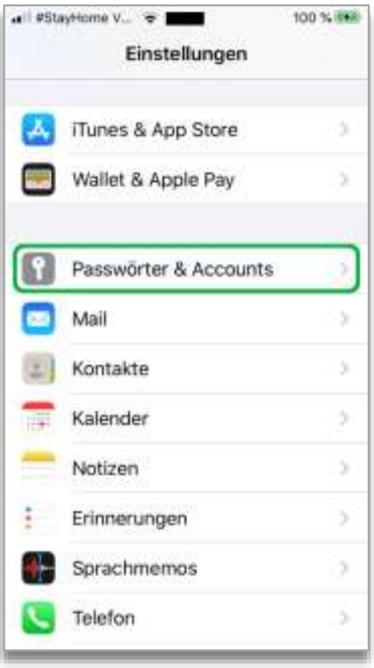
Reinstalling the mail app and re-synchronizing the mails

1. open your appstore and filter for "mail app
2. the familiar mail symbol appears and is marked with a cloud - click on it to download the mail app

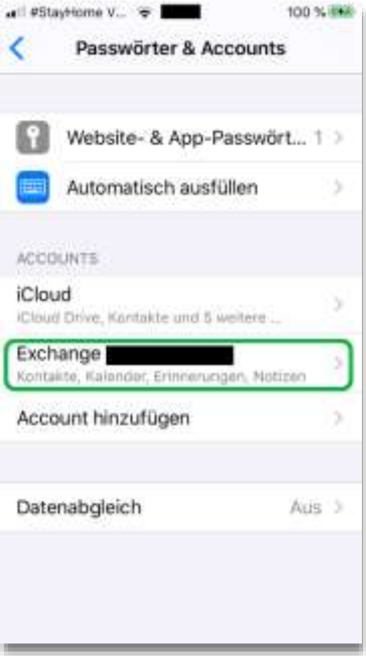


3. Then open the **Passwords & Accounts** section under **Settings**





4. You get a view of all accounts below



#StayHome V... [redacted] 100 %

Passwörter & Accounts

Website- & App-Passwört... 1

Automatisch ausfüllen

ACCOUNTS

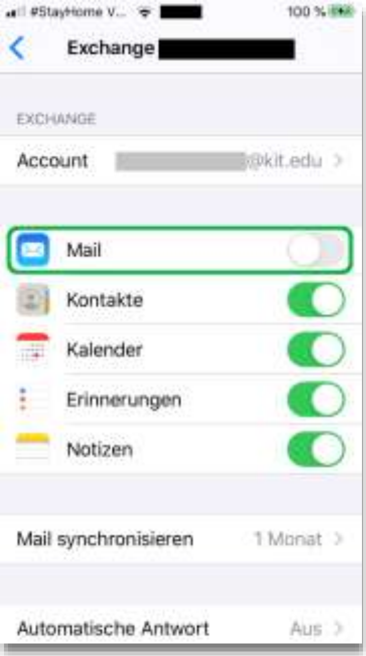
iCloud
iCloud Drive, Kontakte und 5 weitere ...

Exchange [redacted]
Kontakte, Kalender, Erinnerungen, Notizen

Account hinzufügen

Datenabgleich Aus

5. Open the account "Exchange/KIT..." and activate the mails there



#StayHome V... [redacted] 100 %

Exchange [redacted]

EXCHANGE

Account [redacted]@kit.edu

Mail ○

Kontakte ●

Kalender ●

Erinnerungen ●

Notizen ●

Mail synchronisieren 1 Monat

Automatische Antwort Aus

Description of vulerabilities

The iOS app "Mail" is affected by two serious security vulnerabilities on all iOS versions (backdated to iOS 6). Attackers can compromise the iPhone or iPad by sending an email. This potentially makes it possible to read, modify and delete e-mails.Whether further malicious activities are also possible for successful attackers is being checked.
Whether further malicious activities are also possible for successful attackers is being analyzed. The German Federal Office for Information Security (BSI) considers these vulnerabilities to be very critical. No patches are yet available for the two vulnerabilities. According to media reports, the vulnerabilities are already being actively exploited.

Users initially don't notice the attack, except for the possibility that the integrated mail app may run more slowly or be restarted. It is therefore not necessary to actively open the email in iOS 13 to execute the attack. In iOS 12, however, users must actively select the malicious mail for the attack to succeed. Apple changed the way the mail app works with iOS 13; already when receiving a mail, it is downloaded in the background. Therefore, the attack is successful in iOS 13 even without user interaction.
Until patches are available, users should uninstall the "Mail" app on Apple iOS (or alternatively disable the accounts associated with that app).

SOURCES
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Warnung_iOS-Mail_230420.html
https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/

– – –

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