Dear Ladies and Gentlemen,

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

With kind regards
Your SCC Service Team

Cause:
SCC-WARNING – 24.4.2020

SUBJECT
Critical security vulnerability in mail app for iPhone and iPad

NOTE
A serious vulnerability has been found in the standard mail app "Mail" of iOS devices (iPhones and iPads). Mac computers running MacOS are not affected.
According to the recommendations of the BSI, please refrain from using the "Mail" app on iPhones and iPads.

Use of the "Mail" app is temporarily prohibited for devices provided for business purposes.

Procedure: Please temporarily delete the "Mail" app from your device.

For information on how to delete apps from your iPhone or iPad, please visit https://support.apple.com/de-de/HT207618.

If additional mailboxes are connected to the iOS Mail app, make sure that the contents are backed up before deleting the app.

Apple has announced that the vulnerability will be closed with the soon expected security update 13.4.5. We will inform you as soon as the update is available. In addition, we will soon provide you informations on how to reinstall the "Mail" app and put it back into operation.

To continue reading mails on the iPhone or iPads, please use Outlook Web Access at https://owa.kit.edu via a web browser.

RE-INSTALLATION DER MAIL-APP und RESYNCHRONISATION der Mails
Re-installation of the app may only be performed AFTER Apple has provided a security update.

If the mails were accessed via Exchange or IMAP, your mails will be synchronized with the mailboxes again when the app is reconnected.

DESCRIPTION OF VULNERABILITIES
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).

SECURITY UPDATE
Apple has announced that the vulnerability will be closed with the soon expected security update 13.4.5. We will inform you as soon as the update is available. Here we are dependent on Apple.


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