Security Advisory 2022-055

Possible Information Disclosure in MobileIron for Android

July 28, 2022 — v1.0

TLP:WHITE

History:

- 28/07/2022 — v1.0 – Initial publication

Summary

The problem affects Android users using MobileIron and having Use smart send option enabled in Email+ client. When User A forwards/replies email to User B, User B receives a different email body instead of original email.

This could lead to information disclosure especially in case of recipients being outside of the sender’s organisation.

Technical Details

The issue is related to SmartForward/SmartReply. When such feature is in use (offered by Activesync protocol), it allows client to forward messages without retrieving the full, original message from the server on client. Client will send only user's added text and tells Exchange server to send the full text of the original message from server [1].

To do so, client will request Exchange server to look for original email, e.g. with the ServerID X. If somehow ServerID X is used for another email, we will have such issue:

A user of email+ tries to forward email A with serverID X during sync process, after sync email A will have ServerID Y, and ServerID X will be reused for another email B. Since sync is already in progress server thinks that we already use new ServerIDs and forward email B instead of email A.

Affected Products

The following product versions are affected:

- Android email+ all versions
Workaround

To disable SmartForward/SmartReply: From email+ client > settings > disable Use smart send

To disable s_SmartForward/SmartReply_ as a configuration option, you can use the following key/value pairs:

- For email+ version 3.1.1 and higher:
  Use the disabled_features key, and include the value smart_send.

- For email+ version 2.18 and higher:
  Use the enabled_features key, and include the value disable_smart_send.

References