TLS Vulnerability in the Magenta SmartHome App for Android

The Magenta SmartHome-App for Android (https://play.google.com/store/apps/details?id=de.telekom.smarthomeb2c) contains a vulnerability in its implementation of the local TLS TrustManager. For local access to the Qivicon smart home controller via Android smartphones, the Magenta SmartHome app uses a certificate pinning approach. The app uses pre-installed (self-signed) Qivicon root certificates. Only local connections are allowed if the certificate chain leads to one of these pre-installed Qivicon root certificates.

For implementing the certificate pinning approach, the Qivicon implements its own TrustManager (called trust strategy). In particular, the following code appears in the app to implement the trust strategy in the class `AbstractCertificateTrustHandler`:

```
protected boolean checkChain(X509Certificate[] chain) throws
CertificateException {
      if(chain == null) {
            throw new CertificateException("The certificate chain must not
      be null!");
      } else if(chain.length == 0) {
              throw new CertificateException("The certificate chain must
      not be empty!");
      } else {
            boolean isTrusted = false;
            for (X509Certificate checkCertificate : chain) {
                  if(checkCertificate(checkCertificate)) {
                        isTrusted = true;
                  }
            }
             if(isTrusted) {
                  return isTrusted;
             }
            throw new CertificateException("Bad certificate chain! Not
      trusted or issued by a trusted.");

         }
}
```

```
private boolean checkCertificate(X509Certificate cert) throws
CertificateException {
      X509Certificate trustedCertificate;
      cert.checkValidity ();
      for(X509Certificate trustedCertificate2 : this.trustedCertificates) {
            if(trustedCertificate2.equals(cert)){
            return true;
      }
}
```

This code compares the certificate chain array (`chain`) with the array of the pinning certificates `(this.trustedCertificates)` and allows the connection if at least one of the pinning root certificates appears in the array `chain`.

The problem with this code is that now a man-in-the-middle attacker can provide a certificate chain that additionally contains one of the root pinning certs, i.e., the attacker simply adds such a certificate, although it does not belong to the chain (the mitmproxy tool allows one to easily add unrelated certificates to a chain). Then the connection is accepted finally allowing the MITM attack.

Given that the WPA2 vulnerability KRACK may still exist on some Android smartphones as well as on the Qivicon smarthome controller, a MITM attacker can position herself in the proximity of the attacked home and record e.g. credentials to later attack the smart home, for example, open a door or turn off an alarm system.