2020-11 Advisory: CA Certificate Validation on Android devices

Applicable to:

Android 11 QPR1 and beyond.

Introduction

As part of ensuring the Android operating system complies with WPA3 standards (see https://www.wi-fi.org/discover-wi-fi/security [1], and WPA3 Specification v2.0 [2] Section 5), Android will be removing the CA certificate "Do not validate" option in the Wi-Fi EAP settings as of Android 11.

Cause

Certificate validation as part of the EAP protocol in RADIUS is a fundamental security step. It ensures that the certificate presented by the server claiming to be the user's home server is signed by a CA certificate present on the user's device, ensuring that the user's credentials (username and password) are not exposed to a third party attempting a man-in-the-middle (MITM) attack.

In the absence of an EAP network profile that configures a CA certificate, other operating systems such as Apple's iOS use something called 'server certificate pinning' upon first-time connection, in which the server certificate that is presented is 'pinned' and then compared to the certificate presented in subsequent connections.

Android does not have this 'pinning' functionality; and so the Wi-Fi connection instructions that many organisations publish on the internet advise users to select the "Do not validate" option when connecting to their eduroam network. This makes the need for a CA root certificate that has signed the certificate the home server presents to the device, unnecessary. While this speeds up user connection to the eduroam network (by eliminating fiddly steps) and eliminates the requirement to configure user devices specific to the eduroam member organisation, it does so by eliminating an important security step. eduroam(UK) best practice advice is that server certificate validation should never be disabled.

Implications for eduroam

This advisory applies to Android 11 devices and beyond.

As there are eduroam(UK) members who offer Wi-Fi setup instructions that specifically refer

to the "Do not validate" option being selected, this may lead to higher amounts of support requests from December 2020 onwards from users who are using Android 11 devices with QPR1 installed.

eduroam(UK) member organisations using server certificates issued by commercial certificate authorities (including the Jisc Certificate Service) should evaluate whether they are affected by unselecting the "Do not validate" option and then attempt a connection. eduroam(UK) members organisations using server certificates issued by their own internal certificate authorities (our recommended option), unless the CA certificate is already installed on users devices, ***will*** be affected since the CA certificate must be installed on user devices for validation to work.

eduroam(UK) strongly advises that member organisations who do not use the eduroam CAT tool (https://cat.eduroam.org/ [3]) to provide connection profiles for their staff and students, do so to avoid disruption for Android 11 users. We recommend that all members verify and if necessary amend the instructions on their support portals/web pages accordingly and if necessary, provide direct links to their eduroam CAT profiles by logging into the eduroam CAT administrative interface and copying the QR code that is made available in the "Identity Provider download area QR code" section, the link in the same section, or use the geteduroam [4] tool to install the profile directly.

Additional Information

SecureW2's article on Android 11 QPR1: https://www.securew2.com/blog/android-11-server-certificate-validation-error-solution/ [5]

XDA article: https://www.xda-developers.com/android-11-break-enterprise-wifi-connection/ [6]

Reddit thread: https://www.reddit.com/r/networking/comments/j7ero1/psa_android_11s_december_security_update_wi [7]

Links
[1] https://www.wi-fi.org/discover-wi-fi/security
[2] https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf
[3] https://cat.eduroam.org/
[4] https://play.google.com/store/apps/details?id=app.eduroam.geteduroam
[5] https://www.securew2.com/blog/android-11-server-certificate-validation-error-solution/
[6] https://www.xda-developers.com/android-11-break-enterprise-wifi-connection/
[7] https://www.reddit.com/r/networking/comments/j7ero1/psa_android_11s_december_security_update_will/