2021-10 Advisory: Addressing claims of eduroam misconfiguration vulnerability (server certificate validation)

Published: 06/10/2021

This advisory applies to all organisations providing a Home or Home and Visited (Wi-Fi) service.

Recently Jisc, its CSIRT, and the eduroam UK team, as well as the global eduroam community, were made aware of an article on ThreatPost [1] [1] that claimed that some international university Wi-Fi networks could be exposing login credentials through misconfiguration. This article is based on research by WizCase [2] [2], which focuses on the worldwide eduroam wireless network system but also points out that other wireless networks may be similarly affected.

Misconfiguration of any system, IT or otherwise, is likely to compromise its function – imagine servicing your car brakes without bleeding the brake lines. In that sense, an article that flags a problem if people misconfigure their eduroam profile is neither new nor surprising. The valuable contribution that this article makes is noting that some official advice from member organisations actively advocates processes that might lead their staff to a misconfiguration. Specifically in the UK, we aren't aware of any published advice by our members that would fall in this category.

We would like to reassure our members that despite being specifically mentioned in the original disclosure, *eduroam is no more or less affected than any other enterprise Wi-Fi network*. To ensure a secure set-up, there is nothing you need to do for eduroam that you wouldn't already need to do for any other Wi-Fi network that uses the WPA Enterprise (802.1x) standards.

According to the vulnerability map published in WizCase's report, no active eduroam UK sites were highlighted as vulnerable to this risk. While it is true that an 'evil twin' attack is possible, it has limited opportunity:

- This is not a remote attack, so it can only be attempted within close proximity of misconfigured client devices.
- Only client devices which are connecting to the network for the first time, or those where the user has specifically 'forgotten' the eduroam network, would be affected.

There are no reports of this vulnerability being actively exploited.

Apple iOS devices that have accepted the organisation's server certificate on initial connection (otherwise known as Trust On First Use, or TOFU), will 'pin' the server certificate and will

reject server connections where the server certificate fingerprint does not match. This will, in the presence of an 'evil twin', lead to an authentication failure, which in turn may, as indicated above, then lead to the user disconnecting (by 'forgetting' the network connection) and reattempting an authentication. Devices using the Android mobile OS before version 11.0 are offered the opportunity to **not** validate the server certificate. This setting in particular is contentious as it does allow the misconfiguration of Android devices in the manner described by the article.

In both instances, in line with broader global eduroam advice [3] [3], we strongly recommend a combination of the eduroam Configuration Assistance Tool (CAT) and user education to mitigate this risk.

Devices configured with a profile published in the eduroam CAT will **not** be affected as these profiles will contain one or more root certificates, which the profile configures as the only certificate(s) that the server certificate may be validated against. Optionally, a Common Name (CN) is configured that will have to match both the server certificate's CN and subjectAltName data. Additionally, the profile may specify which authentication methods are to be used. If the validation of the certificate (or these parameters) fails, the authentication attempt fails, and no login credentials are exposed.

The article also refers to the use of plain-text credentials inside the EAP (Extensible Authentication Protocol) mechanism, known as PAP (Password Authentication Protocol). PAP is no longer widely used or recommended. The only EAP mechanism to use PAP is EAP-TTLS, whereas the commonly deployed PEAP protocol uses the MSCHAPv2 password mechanism, which, as the article points out, is based on a challenge-response model and is not vulnerable to this risk.

Jisc's eduroam UK operations team, the global eduroam Operations Team and the eduroam National Roaming Operators (NROs) across the world continue to actively encourage sites to adopt best practices for client devices connecting to eduroam. This includes:

- Discontinuing the use of EAP-TTLS/PAP, unless it is absolutely required, and replacing it with alternatives such as EAP-TTLS/MSCHAPv2 or PEAP/MSCHAPv2, or, if the option exists, with EAP-TLS.
- Subscribing your organisation to the eduroam CAT. You can use the CAT to configure standard profiles which your staff and students can use to configure their devices in a consistent way, minimising the risk of misconfiguration. The CAT is completely free to use, please contact the eduroam team [4] [4] if you would like to know more.
- Ensuring that any eduroam guidance offered to staff and students points them to CAT, and explains why it is important to use these profiles, together with the use of the geteduroam app on iOS, Android, and Windows devices.
- Discouraging the use of ad-hoc instructions that limit themselves to TOFU, as well as those which recommend, on versions of Android older than 11, the use of the 'Do not validate' option.
- Adjusting any eduroam documentation to ensure that only eduroam CAT instructions exist.

Jisc would like to encourage all UK eduroam operators who operate a 'Home Only' or 'Home and Visited' service to double-check that their site and server configurations conform with the above best practices. The eduroam team at Jisc would be happy to advise if you are unsure. If any changes are necessary, the operator should also update their information via the eduroam Support Server portal [5] [5] and in their CAT

configuration.

Please contact us at help@jisc.ac.uk [6] if you have any questions or concerns.

Relevant URLs:

1. https://threatpost.com/misconfiguration-university-wifi-login-credentials/175157/ [1]
2. https://www.wizcase.com/blog/eduroam-vulnerability-report/ [2]
3. https://eduroam.org/eduroam-advisory-mutualauth/ [3]
4. https://www.jisc.ac.uk/forms/eduroam-support-request [4]
5. https://support.eduroam.uk/ [5]

Links
[1] https://threatpost.com/misconfiguration-university-wifi-login-credentials/175157/
[2] https://www.wizcase.com/blog/eduroam-vulnerability-report/
[3] https://eduroam.org/eduroam-advisory-mutualauth/
[4] https://www.jisc.ac.uk/forms/eduroam-support-request
[5] https://support.eduroam.uk/
[6] mailto:help@jisc.ac.uk