Advisory: addressing claims of misconfiguration vulnerabilities

Published: 12/10/2021

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

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

As the govroam and eduroam services utilise the same technologies and roaming model, we would like to address the question of whether this threat applies to organisations participating in govroam.

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 profile is neither new nor surprising.

We would like to reassure our members that **govroam 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 govroam that you wouldn't already need to do for any other Wi-Fi network that uses the WPA Enterprise (802.1x) standards.

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 govroam network, would be affected.

There are no reports of this vulnerability being actively exploited.

Managed devices configured with a profile installed via Group Policy or MDM should not be affected as these profiles ought to 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.

Non-managed 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. Non-managed 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.

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 govroam operations team actively encourage sites to adopt best practices for client devices connecting to govroam. 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.
- 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.
- Jisc would like to encourage all UK govroam 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 govroam team at Jisc would be happy to advise if you are unsure.

Please contact us at **govroam@jisc.ac.uk** if you have any questions or concerns.

1)

https://threatpost.com/misconfiguration-university-wifi-login-credentials/175157/

2)

https://www.wizcase.com/blog/eduroam-vulnerability-report/