Advisory: EAP-PWD Vulnerability

Released: 15th April 2019

This advisory is relevant only to eduroam(UK) Home (IdP) (and Home and Visited) service organisations that are supporting the EAP-PWD authentication method – hence will be potentially applicable only to organisations running the FreeRADIUS, Radiator, Aruba ClearPass RADIUS servers or any other servers supporting EAP-PWD (ie not Microsoft NPS). It's aim is to bring to the attention of our community the vulnerability in the EAP-PWD method and describes the position of the Wi-Fi Appliance together with recommend actions to be taken.

Background and scope:

The EAP-PWD vulnerability was discovered by the Belgian researcher Mathy Vanhoef of the University of Leuven and first publicised on 10th April and has received considerable attention, see https://wpa3.mathyvanhoef.com/ [1] Whilst we believe very few member organisations will be affected, this advisory serves to alert any that support EAP-PWD and are not already aware. The FreeRADIUS, Radiator, Aruba ClearPass RADIUS servers and possibly some other servers are capable of supporting EAP-PWD, but Microsoft NPS does not (it primarily supports PEAP/MSCHAPv2). For users to be utilising the EAP method, your ORPS would need to be configured to support it as would the user clients (Android, Windows and wpa_supplicant at least support EAP-PWD).

The Wi-Fi Alliance position is described in the Security Considerations arising from the vulnerability:

https://www.wi-fi.org/file/wpa3-security-considerations [2]

Summary:

Vanhoef's paper about the Dragonfly algorithm used by WPA3 and EAP-PWD can be found here:

https://wpa3.mathyvanhoef.com/ [1]

FreeRADIUS (3.0.19) and OSC (Radiator (4.23)) have released patches for their RADIUS servers already. ClearPass users should check their support vendor's or Aruba's sites.

On the client side, wpa_supplicant is already mostly patched and the following document provides more detailed information about the vulnerability: https://w1.fi/security/2019-2/ [3]

The Wi-Fi Alliance has issued its own response to this vulnerability on the day of disclosure.

Less technical overview: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update-april-2019

[4]

Technical overview: https://www.wi-fi.org/security-update-april-2019 [5]

Security Considerations arising from the vulnerability: https://www.wi-fi.org/file/wpa3-security-considerations [2]

Note the Wi-Fi Alliance does not include EAP-PWD in any of its certification programmes, so the content of the above is centred on the WPA3-Personal (SAE) aspect of the vulnerabilities.

Nonetheless, the Security Considerations document contains some amount of advice for EAP-PWD since it is based on the same underlying algorithm and thus shares significant amount of pertinent security properties.

Action advised:

It is recommended that all affected organisation update their EAP-PWD EAP peers (RADIUS servers and clients).

Links
[1] https://wpa3.mathyvanhoef.com/
[2] https://www.wi-fi.org/file/wpa3-security-considerations
[3] https://w1.fi/security/2019-2/
[4] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update-april-2019
[5] https://www.wi-fi.org/security-update-april-2019