eduroam response to the Blast!RADIUS vulnerability

This advisory is the eduroam response to the attack “Blast!RADIUS - RADIUS/UDP considered harmful” as published on 09 July 2024 at https://blastradius.fail .

Readers are encouraged to read the FAQs on that website and https://www.inkbridgenetworks.com/blastradius/faq prior to reading the details of this advisory.

Conclusions:

- **eduroam authentications are NOT affected by this attack.**
- **Hotspot operators should cautiously check the local administrative access controls for their equipment.**

Observations regarding the attack and its applicability:

1. The attack is focused on and proven to work for most RADIUS authentications which use the PAP, CHAP, and MSCHAPv2 authentication protocols.

- Response 1: eduroam network logins are based exclusively on EAP authentication, so the attack on PAP/CHAP/MSCHAPv2 is not applicable. Note: Many EAP methods carry PAP or MSCHAPv2 as inner authentication payloads inside a TLS tunnel. These uses are protected by TLS encryption, not visible at the RADIUS layer, and not susceptible to the attack.
- Response 2: Where the RADIUS protocol is used to check authentication and authorisation to a device relevant for local eduroam service delivery (be that a Wi-Fi Access Point, controller, or any other piece of network equipment), hotspot operators are advised to proceed with caution and assess the risk for their equipment in regards to the attack, and take appropriate action if necessary. The same considerations as for any other RADIUS client apply; see the FAQ. Reminder: It is a mandatory requirement for eduroam SPs to maintain their equipment according to the specified best practices for security [1].

2. While the paper discusses a possible applicability to EAP authentication, it discusses only EAP authentications in general, and does not go into the details of EAP authentication for Wi-Fi authentication specifically.

- Response: The usage of EAP for Wi-Fi authentication introduces additional protocol elements that are incompatible with the attack vector: An authentication can only succeed if and when the RADIUS server itself generates a dynamic session key from TLS tunnel data and sends that along with the “Accept” response. Even if the attacker can modify a Reject response into an Access-Accept it is not possible for the attacker to craft the correct session key needed by the Wi-Fi process. The Wi-Fi access will thus fail due to missing keying material. eduroam is almost exclusively transacting on Wi-Fi medium, and is thus unaffected on wireless media, even if the attack were to succeed.

3. For EAP authentication on non-Wi-Fi uses of EAP, the paper is inconclusive about the feasibility of the attack. The paper suggests that the attack may succeed in some cases, but they were unable to perform the attack using available software.

- Response: A possible attack on non-Wi-Fi networks (i.e. EAP network authentications which do not require dynamic session keys) would need to exploit a specific implementation detail of a RADIUS/EAP peer; the pertinent RADIUS specification (RFC2869) suggests that implementations “SHOULD” discard messages under the sketched attack circumstances; the attack is only successful if an implementation does not respect this SHOULD. To the best of the knowledge of all key players involved, such an implementation does not exist/is not being used in practice. The niche use of eduroam on wired media (e.g. for wired network ports in student dormitories) is thus also not vulnerable.

[1] https://eduroam.org/wp-content/uploads/2020/02/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf Section 6.2.2