# 2024-07 Advisory: Mitigating Blast!RADIUS by enforcing the use of Message-Authenticator attribute

Released: 9 July 2024

***This advisory is important and relevant to all eduroam(UK) service organisations.***

The eduroam community has been made aware of a recent vulnerability discovered in the RADIUS protocol. This vulnerability, known as Blast!RADIUS and given the CVE number CVE-2024-3596, has been classed with a CVSS score of 9.0.

Importantly however, this vulnerability **does not** affect eduroam traffic as eduroam is based on EAP authentication, albeit transported over the RADIUS protocol. The eduroam community has released a statement about Blast!RADIUS here: https://eduroam.org/eduroam-response-to-the-blastradius-vulnerability/ [1]

eduroam(UK) would also like to note that any RADIUS server (or RADIUS products) that require the use of the Message-Authenticator RADIUS attribute for any RADIUS traffic both on your internal networks and externally to the eduroam national proxy servers will already have made steps forward in mitigating the ability to exploit the vulnerability. Our national proxy servers require the Message-Authenticator attribute to be sent, and also send the Message-Authenticator, as this is a requirement for compliance with the relevant EAP RFC standards.

It is however important that you do check your own settings in your RADIUS server products, and also apply the security patches (or follow security guidance) issued by your RADIUS server vendor to ensure your networks and network devices are not vulnerable.

**Microsoft NPS**

Message-Authenticator settings are by default unset. Administrators can view relevant sections on our eduroam NPS configuration video as follows to ensure they are selected:
For RADIUS clients: https://youtu.be/-7t-_VMJ1tk?feature=shared&t=333 [2]
For RADIUS servers: https://youtu.be/-7t-_VMJ1tk?feature=shared&t=490 [3]

The above time points refer to template entries, but they also apply to the relevant settings in the 'RADIUS Clients' and 'RADIUS Servers' settings.

Microsoft has issued KB5040268, which includes the above information: KB5040268: How to manage the Access-Request packets attack vulnerability associated with CVE-2024-3596 [4]. Please follow Microsoft's advice.

**FreeRADIUS and PacketFence**

Your server configuration should contain the **require_message_authenticator** option set to **yes**

in all your client entries in clients.conf, and all your home_server entries in proxy.conf. The FreeRADIUS project has released a new version of FreeRADIUS that changes the default to **auto**. Please update your version of FreeRADIUS, or update your configuration accordingly.

**Aruba ClearPass (CPPM) and Cisco Identity Services Engine (ISE)**

These should follow the RFCs and to our knowledge do not explicitly expose the Message-Authenticator settings in their UI. If they do, please contact us and we'll correct this advice.

More information about the vulnerability can be found here:

Blast-RADIUS website [5]

Inkbridge Networks [6] (formerly NetworkRADIUS, the makers of the FreeRADIUS server)

Alan DeKok's whitepaper [7]

---



**Links**
[1] https://eduroam.org/eduroam-response-to-the-blastradius-vulnerability/
[2] https://youtu.be/-7t-_VMJ1tk?feature=shared&t=333
[3] https://youtu.be/-7t-_VMJ1tk?feature=shared&t=490
[4] https://support.microsoft.com/en-us/topic/kb5040268-how-to-manage-the-access-request-packets-attack-vulnerability-associated-with-cve-2024-3596-a0e2f0b1-f200-4a7b-844f-48d1d5ab9e66
[5] https://www.blastradius.fail/
[6] https://www.inkbridgenetworks.com/blastradius/faq
[7] https://www.inkbridgenetworks.com/web/content/2557?unique=47be02c8aed46c53b0765db185320249ad873d95