What is subnet router abuse?

A subnet router, or exit node, on a mesh VPN advertises routes to a private network so other nodes can reach hosts behind it. An attacker who controls or enrolls such a node abuses it as an egress relay, routing their traffic through the internal network to reach services and move data while appearing to be internal traffic. Defend by restricting who can advertise and use routes, approving advertised routes, and monitoring relay traffic.

HOW IT WORKS

01 How it works and example

With control of a subnet router or exit node, the attacker routes their traffic through it to reach internal services that are not directly exposed, and uses it as an egress relay so outbound activity looks like normal internal traffic. Combined with a stolen mesh key, this lets an intruder pivot broadly and exfiltrate through a trusted path, as observed in a recent mesh-VPN intrusion.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] HuggingFace, Agent intrusion technical timeline

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/subnet-router-abuse

Open online