

W15D1

Traccia1 :

- Spiegare brevemente cosa vuol dire Null Session • Elencare i sistemi che sono vulnerabili a Null Session • Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni? • Elencare le modalità per mitigare o risolvere questa vulnerabilità • Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

Spiegazione:

Le null session sono delle vulnerabilità presenti in Windows legacy. Si possono sfruttare da remoto, e si possono fare attacchi mediante API o RPC. Sono attacchi che utilizzano la funzione Share del sistema windows senza alcun tipo di autenticazione.

Mitigation:

Aggiornare il sistema operativo all'ultimo pacchetto disponibile, oppure aggiornare a un OS più recente così da non avere più questa vulnerabilità. Togliere l'abilitazione al servizio, ma potrebbe essere controproducente visto che probabilmente l'azienda lo utilizza ogni giorno.