W15D2

NULL SESSION

La traccia

Nella lezione teorica abbiamo visto la **Null Session**, vulnerabilità che colpisce Windows

Traccia

- 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.

Definizione Null Session

La Null Session è una sessione che permette di interagire con un sistema Windows senza dover effettuare l'autenticazione. Tramite la Null Session è possibile ottenere informazioni sul sistema, come l'elenco delle condivisioni e l'elenco degli utenti.
Le "null session" sono un tipo di connessione che permette l'accesso non autenticato a una risorsa di rete su un sistema Windows. In passato, questa vulnerabilità è stata sfruttata in diversi sistemi Windows, in particolare nelle versioni più vecchie del sistema operativo.

Versioni di Windows vulerabili

Le versioni di Windows più note per essere vulnerabili alle "null session" includono:

1. **Windows NT**: Questa versione di Windows è stata una delle prime a presentare la vulnerabilità delle "null session". I sistemi Windows NT 4.0 e versioni precedenti erano particolarmente suscettibili.
2. **Windows 2000**: Anche Windows 2000 è stato noto per essere vulnerabile alle "null session".
3. **Windows XP**: In passato, Windows XP ha avuto problemi legati alle "null session", soprattutto nelle versioni non aggiornate.
4. **Windows Server 2003**: Anche questa versione del sistema operativo Windows è stata soggetta a problemi legati alle "null session".
5. **Windows Vista, 7, 8, e 8.1**: Anche se meno suscettibili rispetto alle versioni più vecchie, queste versioni di Windows potrebbero presentare vulnerabilità alle "null session" se non sono aggiornate con le patch di sicurezza più recenti.

Solution

Dove possibile si può semplicemente applicare una patch per tale vulnerabilità, in alternativa andrebbe aggiornato il sistema operativo delle macchine interessate.