Ipotesi di Remediation per MS17-010

1. Possiamo risolvere in qualche modo? Se sì, con quale sforzo?

Sì, la vulnerabilità MS17-010 può essere risolta. Lo sforzo dipende dall'approccio:
- Patch ufficiale Microsoft: Sforzo basso-medio. Microsoft ha rilasciato patch di sicurezza per questa vulnerabilità nel marzo 2017. L'applicazione richiede il download e l'installazione dell'aggiornamento, seguito da un riavvio del sistema.
- Workaround temporanei: Sforzo medio. Se il patching immediato non è possibile, si possono implementare soluzioni temporanee come la disabilitazione di SMBv1.

2. Possiamo risolvere solo la vulnerabilità?

Sì, la patch elimina specificamente la vulnerabilità MS17-010, ma non risolve il problema strutturale se:
- SMBv1 rimane abilitato,
- i sistemi non vengono aggiornati regolarmente,
- non esistono controlli di rete e segmentazione.

Una remediation limitata alla sola patch riduce il rischio immediato, ma non protegge da exploit simili futuri né da altre vulnerabilità del servizio SMB.
Per una remediation corretta è quindi raccomandato:
- disabilitare SMBv1 ove non strettamente necessario,
- mantenere policy di patch management continuative,
- verificare configurazioni legacy ereditate.

3. Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

Sì, ed è un punto fondamentale.
Anche nel caso in cui un attaccante riesca a sfruttare MS17-010 su un host, è possibile limitare drasticamente l’impatto tramite controlli difensivi aggiuntivi:
- Segmentazione di rete: impedire la comunicazione SMB indiscriminata tra host.
- Restrizioni firewall: limitare l’accesso alla porta 445 solo ai sistemi che ne hanno reale necessità.
- Least Privilege: ridurre privilegi amministrativi locali e di dominio.
- Monitoraggio: rilevare exploit SMB e movimenti laterali anomali.
- Disabilitazione di SMBv1: elimina il vettore di propagazione utilizzato da EternalBlue e malware come WannaCry.

Queste misure non correggono la vulnerabilità, ma contengono l’attacco, riducono la superficie di propagazione e aumentano le possibilità di detection precoce.