

Esercitazione WEEK 17 D1

Hacking Windows XP Remediation

Ettore Farris

Descrizione sintetica

Formulare delle ipotesi di remediation della vulnerabilità MS08-067. Ad esempio:

- **1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se sì, con quale effort?**

L'attacco colpisce Microsoft Windows 2000, Windows XP, Windows Server 2003 e può essere risolto facendo un aggiornamento di sicurezza.

- **2. L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?**

La vulnerabilità potrebbe consentire l'esecuzione del codice remoto se un sistema interessato ha ricevuto una richiesta RPC appositamente creata. L'aggiornamento della sicurezza risolve la vulnerabilità correggendo il modo in cui il servizio Server gestisce le richieste RPC. Se la vulnerabilità è presente, Microsoft consiglia ai clienti di applicare immediatamente l'aggiornamento.

- **3. Una volta dentro l'attaccante, può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?**

La problematica può essere risolta ed esempio attivando il firewall e aggiornando il sistema.

