PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1145 di venerdì 17 dicembre 2004

"Regali di Natale" da Microsoft

Rilasciate 5 nuove patch per eliminare diverse vulnerabilità riscontrate in Windows.

Pubblicità

Dopo la importante patch rilasciata all'inizio di dicembre per eliminare la pericolosa vulnerabilità in Internet Explorer, Microsoft ha reso note negli ultimi giorni altre cinque nuove patch a correzione di bachi riscontrati in alcuni prodotti.

Nel bollettino MS04-041 viene descritta la vulnerabilità presente in WordPad, noto editor testuale, che se sfruttata può consentire l'esecuzione di codice non autorizzato da parte di un assalitore.
"Se un utente è connesso con privilegi amministrativi, un pirata informatico che sfrutta queste vulnerabilità - precisa il bollettino - può assumere il pieno controllo di un sistema interessato ed eseguire operazioni quali l'installazione di programmi, la visualizzazione, la modifica o l'eliminazione di dati e la creazione di nuovi account con privilegi completi. Pertanto gli utenti con account configurati in modo da disporre solo di privilegi limitati sono esposti all'attacco in misura inferiore rispetto a quelli che operano con privilegi amministrativi. Per poter sfruttare questa vulnerabilità è tuttavia necessaria l'interazione dell'utente."
Microsoft consiglia l'immediata applicazione della patch a tutti gli utenti Windows.

Anche la vulnerabilità riscontrata nel Windows Internet Naming Service (WINS) e descritta nel bollettino MS04-045 può consentire, se opportunamente sfruttata, l'esecuzione di codice in modalità remota.

E' classificato come "importante" anche il livello di gravità delle vulnerabilità descritte nei bollettini MS04-042, MS04-043, MS04-044.
Il primo fornisce la patch per eliminare una vulnerabilità, in DHCP (Dynamic Host Configuration Protocol), che può consentire l'esecuzione di codice in modalità remota e la negazione del servizio.
Nel bollettino MS04-043 è descritta una vulnerabilità contenuta nel componente HyperTerminal di Windows legata all'esecuzione di codice in modalità remota a causa di un sovraccarico del buffer, che può consentire l'esecuzione di codice non autorizzato.
Mentre nel bollettino MS04-044 vengono descritte vulnerabilità del kernel di Windows e LSASS che possono consentire l'acquisizione di privilegi più elevati.
