PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1162 di martedì 18 gennaio 2005

Patch per la sicurezza

Microsoft rilascia i primi bollettini di sicurezza dell'anno. Individuate vulnerabilità critiche.

Primi tre bollettini di sicurezza del 2005, con relative patch, per i prodotti Microsoft.

La rassegna mensile delle vulnerabilità si è aperta con un baco presente in HTML Help che, se abilmente sfruttato, può consentire l'esecuzione di codice non autorizzato e l'intercettazione di informazioni personali.
Il bollettino MS05-001 informa che se un utente è connesso con privilegi amministrativi, un assalitore che riesca a sfruttare questa vulnerabilità, presente nel controllo ActiveX di HTML Help in Windows, potrebbe assumere il controllo completo del sistema interessato, riuscendo a installare programmi e a visualizzare, modificare o eliminare dati oppure a creare nuovi account con privilegi amministrativi.
Microsoft, definendo il baco "critico", raccomanda l'immediata applicazione della patch.

Di livello "critico" è anche la vulnerabilità per i sistemi Windows, descritta nel bollettino MS05-002, individuata nella gestione dei formati dei cursori e delle icone.
Un hacker potrebbe sfruttare la vulnerabilità creando un cursore o un'icona dannosi in grado di consentire l'esecuzione di codice in modalità remota, se un utente visita un sito Web dannoso o visualizza un messaggio di posta elettronica dannoso. Se la vulnerabilità viene sfruttata può consentire a un assalitore di assumere il controllo completo del sistema interessato.

Meno grave è invece il baco individuato in Windows nel servizio di indicizzazione e reso noto nell'ultimo bollettino emesso.
Si tratta di una vulnerabilità legata all'esecuzione di codice in modalità remota. Se la vulnerabilità viene sfruttata può consentire a un hacker di assumere il controllo completo del sistema interessato. Esistono tuttavia significativi fattori attenuanti che consentono di ridurre la gravità di questa vulnerabilità.
