PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 817 di lunedì 14 luglio 2003

Patch per Windows

Individuate tre falle di sicurezza, una delle quali definita "critica". Come correggerle.

Con tre bollettini di sicurezza Microsoft ha reso note tre nuove falle di sicurezza in Windows, per una delle quali il livello di gravità è stato definito "critico".
Il grave baco, descritto nel bollettino MS03-023, è presente nelle modalità con cui il convertitore HTML di Microsoft Windows (che permette di visualizzare, importare o salvare file in formato HTML) gestisce una richiesta di conversione durante un'operazione di copia e incolla nel supporto per la conversione HTML.

Tale vulnerabilità può essere sfruttata per compromettere la sicurezza del sistema. "L'invio al convertitore HTML di una richiesta opportunamente predisposta può provocare l'esecuzione di codice nel contesto dell'utente connesso al sistema.

Poiché questa funzionalità è utilizzata da Internet Explorer, l'autore dell'attacco può creare una pagina Web o un messaggio di posta elettronica HTML in grado di utilizzare il convertitore HTML per l'esecuzione di codice non autorizzato sul sistema dell'utente. L'utente può consentire a un hacker di sfruttare questa vulnerabilità semplicemente visitando il suo sito Web". Microsoft consiglia agli amministratori di sistema di applicare immediatamente la patch.

Il livello di gravità delle due altre vulnerabilità, descritte rispettivamente nei bollettini MS03-024 e MS03-025, è "importante".

La prima riguarda Windows NT, Windows 2000 o Windows XP; sfruttando questa vulnerabilità un utente malintenzionato potrebbe provocare la sovrascrittura di aree casuali della memoria, provocando in tal modo il danneggiamento dei dati o un errore del sistema oppure consentendo l'esecuzione di codice non autorizzato.

Per attuare l'attacco, tuttavia, l'aggressore deve disporre di un nome utente e di una password validi, per poter essere autenticato dal server.

La seconda vulnerabilità riguarda solo Windows 2000.
Sfruttando questa vulnerabilità, un assalitore può ottenere privilegi a cui non ha diritto. In questo caso, l'autore dell'attacco può ottenere privilegi amministrativi completi, che gli consentono di eseguire qualsiasi azione sul sistema, come aggiungere, eliminare o modificare i dati contenuti, creare o eliminare account utente e aggiungere account al gruppo degli amministratori locali.

Anche per quest'ultime vulnerabilità è consigliata l'installazione delle patch che si trovano nei relativi bollettini di sicurezza.
