PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1083 di lunedì 20 settembre 2004

Attacchi informatici...via immagini

Microsoft rilascia una serie di aggiornamenti per eliminare una vulnerabilità contenuta in un componente per la gestione delle immagini.

Interessa numerosi programmi e componenti la grave falla di sicurezza segnalata da Microsoft, relativa al processo dell'elaborazione delle immagini in formato JPEG. Sfruttando questa vulnerabilità, un pirata informatico può assumere pieno controllo di un sistema interessato ed eseguire operazioni quali l'installazione di programmi, la visualizzazione, la modifica o l'eliminazione di dati.

Ad essere colpiti dalla vulnerabilità vi sono, ad esempio, i sistemi operativi Microsoft Windows XP, Microsoft Windows XPService Pack 1, Windows Server 2003, in quanto contengono il componente esposto a questa vulnerabilità per impostazione predefinita.
Le versioni precedenti di Windows non presentavano una versione di questo componente associata al sistema operativo. Tuttavia il componente esposto alla vulnerabilità può venire installato su questi sistemi operativi durante l'installazione di programmi o componenti. Tra i software esposti alla vulnerabilità vi sono anche i diffusissimi programmi di Microsoft Office XP , Microsoft Office 2003 (es. word, excel, Outlook, internet explorer), Project 2002 a Visio 2003. [L'elenco completo dei software vulnerabili è consultabile nel bollettino di sicurezza]. Possono inoltre essere esposte alla vulnerabilità anche software non di Micorsoft che eseguono l'elaborazione dei file JPEG, le applicazioni di terze parti sviluppate mediante Visual Studio .NET 2002, Visual Studio .NET 2003 o Microsoft .NET Framework versione 1.0 SDK Service Pack 2 e le applicazioni di terze parti che distribuiscono la propria copia del componente interessato

Numerose le modalità con le quali un pirata informatico potrebbe cercare di sfruttare questa vulnerabilità. Un hacker, ad esempio, potrebbe progettare un sito Web per sfruttare la vulnerabilità tramite Internet Explorer 6 e quindi indurre un utente a visualizzare il sito, oppure creare un messaggio di posta elettronica HTML con un'immagine allegata appositamente predisposta. L'immagine potrebbe essere progettata per sfruttare la vulnerabilità tramite Outlook 2002 o Outlook Express 6.
Il pirata informatico potrebbe anche incorporare un'immagine appositamente predisposta in un documento Office e quindi indurre l'utente a visualizzare il documento.

Microsoft ha reso disponibili gli aggiornamenti, disponibili nel bollettino di sicurezza, per eliminare la vulnerabilità dai prodotti che ne sono interessati e ne raccomanda l'immediata applicazione.
Se sul computer sono stati installati programmi o componenti esposti alla vulnerabilità, è necessario installare l'aggiornamento per la protezione richiesto per ciascuno dei programmi o componenti interessati.

---

www.puntosicuro.it