PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1180 di venerdì 11 febbraio 2005

Microsoft fa il pieno di...patch

Rilasciati 12 nuovi aggiornamenti di sicurezza per i suoi prodotti.

Un lungo elenco di bollettini di sicurezza è stato rilasciato da Microsoft del mese di febbraio. Comunicazioni che descrivono vulnerabilità scoperte di recente in Windows e in alcuni programmi.
In particolare il bollettino MS05-014 contiene un aggiornamento cumulativo, definito critico, per la protezione di Internet Explorer che risolve inoltre varie vulnerabilità scoperte di recente.

I bollettini MS05-015, MS05-013, MS05-011, MS05-010, MS05-008, MS05-007 sono indirizzati ai clienti che utilizzano Microsoft Windows e descrivono varie vulnerabilità che, se opportunamente sfruttate da pirati informatici, possono consentire l'esecuzione di codice in modalità remota o, come per la vulnerabilità descritta in MS05-013, l'intercettazione di informazioni personali, oppure l'esecuzione di codici non autorizzati.
Microsoft raccomanda l'installazione delle relative patch indicate nei bollettini di sicurezza.

Il bollettino MS05-012 si rivolge invece ai clienti che utilizzano Microsoft Windows, Microsoft Exchange Server, Microsoft Office o applicazioni di terze parti che utilizzano la tecnologia OLE.
Microsoft raccomanda al più presto l'installazione delle relative patch.

Una vulnerabilità presente nel processo delle immagini PNG (che può consentire l'esecuzione di codice in modalità remota) è stata descritta nel bollettino MS05-009, rivolto ai clienti che utilizzano Microsoft Windows Media Player, Windows Messenger e MSN Messenger.

Ai clienti che utilizzano Microsoft Windows SharePoint Services o SharePoint Team Services di Microsoft è invece indirizzato il bollettino sulla sicurezza MS05-006 che descrive una vulnerabilità che potrebbe essere sfruttata da un hacker per indurre un utente a eseguire uno script dannoso.
Nel bollettino è indicato come installare la patch per eliminare tale vulnerabilità.

Il bollettino MS05-005 descrive un baco presente in Microsoft Office XP, associato all'esecuzione di codice in modalità remota in un sistema interessato. Sfruttando questa vulnerabilità, un hacker potrebbe assumere pieno controllo del sistema interessato. Micorsoft raccomanda agli utenti che utilizzano Microsoft Office XP, Microsoft Project 2002, Microsoft Visio 2002 o Microsoft Works Suite di installare la relativa patch.

Il bollettino MS05-004, indirizzato ai clienti che utilizzano Microsoft Windows .NET Framework, descrive una vulnerabilità nella convalida dei percorsi in ASP.NET, che potrebbe consentire a un hacker di aggirare le difese di un sito Web ASP.NET per ottenere l'accesso non autorizzato e l'intercettazione di informazioni personali.
