PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 959 di venerdì 12 marzo 2004

Microsoft rende note nuove vulnerabilita'

Falle di sicurezza sono state individuate in Windows, Office e MSN Messenger. Disponibili le patch.

Sono tre le nuove vulnerabilità rese note da Microsoft, delle quali tuttavia nessuna è stata classificata al massimo livello di criticità ("critical").

La prima falla, descritta nel bollettino MS04-008, riguarda i Servizi Windows Media componente server di Windows 2000 che consente di trasmettere contenuto da un server Windows Media ai client Windows Media in Internet o in un'Intranet. I clienti che ricevono il contenuto possono riprodurlo o visualizzarlo nel momento stesso della ricezione senza prima doverlo scaricare.
La vulnerabilità, del tipo di negazione del servizio, se sfruttata da un hacker, può impedire al servizio di Stazione o di Monitoraggio di Windows Media, in esecuzione in un sistema Windows 2000 Server, di rispondere alle nuove richieste.
Microsoft consiglia agli amministratori di sistema di applicare al più presto l'aggiornamento di sicurezza, disponibile sul sito, ai sistemi che eseguono Windows 2000 e in cui sono installati i Servizi Windows Media 4.1.

Il secondo bollettino pubblicato nel mese di marzo si rivolge invece a coloro che utilizzano Microsoft Office XP e/o Outlook 2002.
La vulnerabilità descritta, con livello di criticità "importante", è infatti presente in Outlook 2002, programma disponibile sia come prodotto autonomo, sia come parte di Office XP.
La vulnerabilità causa l'acquisizione di privilegi più elevati; l'autore di un attacco potrebbe sfruttarla per indurre Internet Explorer a eseguire script nel contesto di protezione dell'area del Computer Locale del sistema interessato. Sfruttando questa vulnerabilità un hacker potrebbe accedere ai file ed eseguire codice non autorizzato nel sistema dell'utente.

L'ultima vulnerabilità, di gravità "moderata", è descritta nel Bollettino MS004-010 ed interessa il servizio Microsoft MSN Messenger.
Si tratta di una vulnerabilità di accesso a informazioni personali. Sfruttando questa falla l'autore dell'attacco ha la possibilità di visualizzare il contenuto di un file presente sul disco rigido all'insaputa dell'utente, se ne conosce la posizione esatta.
L'utente legittimo non ha modo di sapere che un utente non autorizzato sta tentando di leggere i file.
