Pericolo vulnerabilità in ActiveX Data Objects

30/10/06

Su una delle più famose Bugtraq del web, SecurityFocus, è stata segnalata una vulnerabilità che se sfruttata tramite Internet Explorer 6 potrebbe compromettere il funzionamento dell'intero sistema. Microsoft ha già confermato l'esistenza di tale falla e sta già lavorando per una soluzione. Al Microsoft Security Response Center Blog hanno rilasciato un post in cui si conferma la presenza di una falla di sicurezza relativa al ActiveX Data Object. Ma non si conferma che tale exploit rilasciato sia in grado di sfruttarla ed eseguire codice da remoto, come dichiarato. Per tanto il Team di sicurezza di Microsoft è al lavoro per capire il reale pericolo.Tale bug potrebbe essere sfruttato da un utente malintenzionato per eseguire codice arbitrario da remoto creando una apposita pagina HTML da far visualizzare alla vittima tramite IE 6.Il pericolo è da prendere sul serio, in quanto oltre all'avviso di sicurezza rilasciato alla Bugtraq SecurityFocus a questo indirizzo: http://www.securityfocus.com/bid/20704, è stato rilasciato anche l'exploit in grado di sfruttare il bug. Ovviamente il PoC (Proof of Concept, NDR) rilasciato è solamente indicativo per dimostrare la vulnerabilità.L'exploit, cioè il codice per sfruttare tale vulnerabilità, è veramente semplice da creare ed è composto da pochissime righe. La frase che mi ha colpito è stata la seguente (presente sul PoC):

 It`s will be fast with some shellcode.Cioè: "Sarà veloce come una shellcode". Per chi è del settore questa frase significa solamente che l'esecuzione di codice da remoto è molto semplice e veloce da costruire.I dati tecnici della vulnerabilità spiegano come il problema sia localizzato nella funzione ActiveX Object "ADODB.Connection.2.7", causando una corruzione di memoria che porta ad un crash della macchina stessa.L'autore dell'avviso ha segnalato come vulnerabile tutte le versioni di Microsoft Windows con tutti gli aggiornamenti di sicurezza sino ad ora rilasciati e il browser Internet Explorer versione 6.

fonte: www.orebla.it
link: http://www.orebla.it/module.php?n=news_301006_2