

Windows XP minacciato dal tasto F1

- Ultima modifica: Mercoledì, 03 Marzo 2010 13:21

Pubblicato: Mercoledì, 03 Marzo 2010 13:21

Scritto da Laura Benedetti



Un bug in VBScript può essere sfruttato allo scopo di eseguire codice arbitrario da remoto. Si tratta di una vulnerabilità relativa a Internet Explorer in Windows XP, dopo aver premuto il tasto F1.

Un ricercatore di sicurezza informatica polacco, Maurycy Prodeus, ha comunicato la sua scoperta sul Web. Secondo lui, è possibile eseguire **winhlp32.exe** da **Internet Explorer 6, 7 e 8** allo scopo di utilizzare **VBScript** per l'attivazione di un file d'aiuto (estensione .hlp) malevolo. Questa falla, che permetterebbe quindi l'esecuzione di codice arbitrario da remoto, è presente solo su **Windows XP** ma non su Windows Vista o Windows 7. La vulnerabilità è stata in realtà scoperta il 1° febbraio 2007 e solo lo scorso 26 febbraio è stata portata nuovamente all'attenzione dei media.



Windows XP minacciato dal tasto F1

- Ultima modifica: Mercoledì, 03 Marzo 2010 13:21

Pubblicato: Mercoledì, 03 Marzo 2010 13:21

Scritto da Laura Benedetti

Per l'esecuzione del codice arbitrario, è richiesta l'interazione dell'utente che deve **premere il tasto F1** con la visualizzazione di una finestra di dialogo. La società Secunia ha confermato che la vulnerabilità 0-day è presente almeno su IE7 e Windows XP SP3. Il bug sembra essere dovuto ad un errore nel funzionamento **MsgBox () di VBScript** e può essere sfruttato "per eseguire un file HLP a distanza, suggerendo all'utente di premere il tasto F1 nel corso della consultazione di un sito Web malevolo".

Questo intervento dell'utente porta la vulnerabilità ad un livello di **pericolo medio**. Microsoft ha indicato di essere già impegnata nella ricerca della vulnerabilità, nelle sue cause e conseguenze. "Al momento", chiarisce Microsoft, "nessun attacco ha interessato sistemi operativi Windows Vista e Windows 7 (e Windows Server 2008 e 2008 R 2)".