Windows kernel GDI pericolosamente vulnerabile

07/11/06

È stata segnalata una vulnerabilità che affliggerebbe una parte del Kernel di Windows, relativamente alle GDI. Questo bug sarebbe stato scovato e segnalato da un Blog il quale si occupa ogni mese di rilasciare le procedure, i dettagli e gli exploit corretti per sfruttare le vulnerabilità da loro trovate nei kernel dei vari sistemi operativi.Il gruppo (se così si può definire) si chiama Month of Kernel Bugs, più semplicemente MOKB, ed è come un Bug Traq però entra molto nello specifico. Infatti spiega in modo dettagliato come utilizzare l'exploit associato a tale vulnerabilità con tutti i passaggi.Sicuramente il MOKB è una iniziativa che permette di rendere più sicuro il sistema operativo, in quanto si occupa di ispezionare il cuore del SO, altro non è che il kernel.Anche se la spiegazione in dettaglio su come sfruttare la falla potrebbe avere riscontri non positivi, ma potrebbe anche velocizzare il rilascio di eventuali aggiornamenti.Potete trovare maggiori dettagli sul MOKB a questo indirizzo: http://projects.info-pull.com/mokb/.La vulnerabilità in questione, quella relativa al Microsoft Windows kernel GDI è stata scovata circa 2 anni fa e allo stesso tempo segnalata a Microsoft. Attualmente però nulla è stato rilasciato dai tecnici Microsoft per tappare tale falla.Così il MOKB oltre a segnalare i dettagli della vulnerabilità, che esamineremo in seguito, ha anche messo a disposizione l'exploit e il relativo debug per poter capire il funzionamento di tale falla.In dettagli il problema sarebbe relativo ad un blocco di scrittura che non viene effettuato dal kernel. Infatti l'utilizzo di oggetti GDI è possibile tramite chiavi di sola-lettura nella memoria, una porzione di codice però non blocca la possibilità di trasformare questa "lettura" in "scrittura". Dando la possibilità ad un file eseguito sul PC vittima di scrivere sulla memoria con tutti i permessi necessari per prendere possesso della macchina.Anche Secunia ha localizzato tale bug ma lo ha classificato solamente come "Poco Critico", potete visualizzare l'advisory di Secunia a questo indirizzo: http://secunia.com/advisories/22668/.

fonte: www.orebla.it
link: http://www.orebla.it/module.php?n=news_071106_3