Betriebssystem Vista schon geknackt

Beitrag von „darkdiver“ vom 7. August 2006 um 19:16

Microsoft hat die Schwachstelle bereits geschlossen :trinken

Ist auch kein wirklicher Hack, ist eher ein logischer Fehler in der Revision welche verteilt wurde. Es gab für diesen Mechanismus keine Sicherheitsvorkehrung. Von Hacken kann nur dann die Rede sein wenn eine Sicherheitsvorkehrung überlistet wurde.

Das wäre ja fast so, als wäre bereits das Ansehen einer Platte schon ein Versuch sie zu hacken...:D

Die haben das ganz einach gemacht:

Schritt 1:
die haben ein Programm geschrieben, welches so viel RAM vom System angefragt hat, dass dieses die signierten Treiber aus dem Speicher auf die Platte ausgelagert hatte
Schritt 2:
dann geht das Programm dort in der PAGEFILSYS hin und manipuliert diese Treiber bzw. tauscht diese aus.
Schritt 3:
Dann geben sie den Speicher wieder frei
Schritt 4:
dann lädt das System diesen Bereich wieder von der Platte wieder in den RAM und schwups ist der unsignierte und vor allem korrumpierte Treiber im Kernel.

Aber damit kann die Presse sehr beeindruckt werden und es kommen solche Meldungen auf

Nun es ist immer so, viele Leute sehen Hacks und Hacker wo keine Sinn, denn echte Hacker sieht keiner, nur deren Auswirkung .

Regel Nr.1 eines Hacker hinterlasse keine Hinweise nach deinen Besuch bzw. hinterlasse falsche

Regel Nr.2 Tausche einen Angriff auf ein System an Feature "A" vor um ein Feature "B" zu kompromitieren. Dann wird der Admin den Fehler "A" finden und beheben und "B" erst garnicht vermuten.

Regel Nr.3 Lass den Admin den Fehler selbst erzeugen und den Trojaner selbst einschleusen. (siehe Schritt 3+4)

Und so weiter...

Wenn es jemanden Interessiert, kann ich ein wenig mehr hier zum Thema IT und TK Sicherheit.

Viele Grüße
Eric

wer einmal sehen will was auf seinem Windows Rechner alles los ist. z.B. welche Dienste oder Netzwerktreiber geladen wurden...

http://www.sysinternals.com/Utilities/Autoruns.html

Viele Grüße
Eric