Betriebssystem Vista schon geknackt

Beitrag von „Thanandon“ vom 7. August 2006 um 18:30

Na das fängt ja schon gut an....
==========
Eigentlich soll das nächste Microsoft-Betriebssystem sehr sicher werden. IT-Experten haben nun demonstriert, wie man den XP-Nachfolger hacken kann.

Das neue Windows Vista Betriebssystem konnte auf der Hackerkonferenz Black-Hat in Las Vegas geknackt werden, wie der Fachdienst „Informationweek“ berichtet. Joanna Rutkowska, Sicherheitsexpertin des Singapurer Security-Unternehmens Coseinc, demonstrierte, dass sich die Sicherheitsvorkehrungen trotz Verbesserungen umgehen lassen. So werden in der 64-Bit-Version unsignierte Treiber blockiert, um zu verhindern, dass schädlicher Code tief in das System eindringt.

Doch obwohl Windows viel Arbeit in die Verbesserung der Sicherheit investierte, gelang es Rutkowska ungeprüften Code einzuschleusen und auszuführen. Produktmanagement-Direktor Austin Wilson von Microsoft betonte allerdings gegenüber Journalisten, dass für diesen Hack Administratorenrechte notwendig seien.

„Vista nicht völlig unsicher“

„Die Tatsache, dass der Mechanismus umgangen werden kann, bedeutet nicht, dass Vista völlig unsicher ist. Es ist nur nicht so sicher wie in der Werbung versprochen“, relativierte Rutkowska die Sicherheitsmängel. Hundertprozentige Sicherheit könne ohnehin nicht garantiert werden, da Hacker immer einen Weg fänden, sich ins System einzuschleichen.

Wilson nahm die geglückte Hack-Attacke scheinbar gelassen. „Genau das ist der Grund, warum wir hier sind“, meinte er gegenüber Journalisten. Nach Rutkowskas Demonstration zeigte sie noch einige Möglichkeiten, dieser Attacke gegenzusteuern.

Microsoft will die Schwachstelle schließen

Microsoft gibt an, bereits eine Möglichkeit gefunden zu haben, diese Sicherheitslücke zu schließen. Die Auslieferung des Betriebssystems werde deswegen jedenfalls nicht verzögert. Auf der Hacker-Konferenz verteilte der Konzern bereits Preview-Versionen des Vista-Betriebssystems.

Zu Beginn des kommenden Jahres, wenn Vista in die Läden kommt, sollen alle Mängel behoben sein. Das Feedback von Sicherheitsexperten soll helfen, die Sicherheitseinstellungen vor der endgültigen Veröffentlichung weiter zu verbessern.

Quelle

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

Beitrag von „jome“ vom 7. August 2006 um 21:01

> Zitat von darkdiver
>
> 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
>
> Alles anzeigen

Der ProcessExplorer von Sysinternals ist da auch empfehlenswert

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

Nur schade daß die Firma von Symantec gekauft wurde. Nach allen bisherigen Erfahrungen werden die auch die Programme von Sysinternals eklatant "verbessern" 

Beitrag von „agroetsch“ vom 8. August 2006 um 10:43

> Zitat von jome
>
> Der ProcessExplorer von Sysinternals ist da auch empfehlenswert
>
> http://www.sysinternals.com/Utilities/ProcessExplorer.html
>
> Nur schade daß die Firma von Symantec gekauft wurde. Nach allen bisherigen Erfahrungen werden die auch die Programme von Sysinternals eklatant "verbessern" 

Hallo,

das Programm ist klasse, das benutze ich immer um zu sehen welche Task noch eine bestimmte Datei im Zugriff hat. Sehr nützlich!

Beitrag von „TouaregAti“ vom 8. August 2006 um 12:50

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

Aha, Du kommst auch aus der IT-Ecke? Gibt´s hier noch mehr von uns? :trinken

---

Beitrag von „darkdiver“ vom 8. August 2006 um 13:33

> Zitat von TouaregAti
>
> Aha, Du kommst auch aus der IT-Ecke? Gibt´s hier noch mehr von uns? :trinken

Hi,

was machst du und wo ?

Grüße
Eric

Beitrag von „TouaregAti“ vom 8. August 2006 um 13:42

> Zitat von darkdiver
>
> was machst du und wo ?

Bin gelernter Büroinformationselektroniker, habe mich auf PCs und die Rundum-Betreuung kleiner und mittlerer Unternehmen zwischen München und Salzburg spezialisiert. Mittlerweile mache ich einen Teil meines Umsatzes mit Web-Seiten (PHP, MySQL, ...). Und Du?

Ciao

Ati

Beitrag von „darkdiver“ vom 8. August 2006 um 14:01

hmm, ich würde es am besten mit Projektleiter bei Arcor für Endgeräte im Bereich Wlan Router, Modems und IADs beschreiben. Ich Kümmere mich im Moment um das Thema VoIP als firstline Service und NGN Softswitch.

Ich habe davor lange Jahre Firewallsysteme und Managed Firewall Services für Key Accounts von Arcor gemacht. z.B. Kultusministerium in BW etc.

Privat mache ich viel mit PHP und MySQL für die Touareg-Freunde

Viele Grüße
Eric

Beitrag von „TouaregAti“ vom 8. August 2006 um 15:55

> Zitat von darkdiver
>
> Ich habe davor lange Jahre Firewallsysteme und Managed Firewall Services für Key Accounts von Arcor gemacht. z.B. Kultusministerium in BW etc.
>
> Privat mache ich viel mit PHP und MySQL für die Touareg-Freunde

"Firewall? Brauchen wir nicht. Wir haben keine Probleme mit Viren und dergleichen,

...

...

...

aber mein PC ist im Internet seit zwei Wochen so langsam ..."

Das war ein O-Ton Kunde. Den Rest kann man sich denken ...

Übrigens, mein neues "Freizeit-Projekt" (mehr oder weniger), seit gestern online: http://www.erdoelfrei.de

(Muss darauf achten, dass für meinen V8 genug Öl übrig bleibt)

Beitrag von „Hagen“ vom 8. August 2006 um 17:44

> Zitat von jome
>
> ...Nur schade daß die Firma von Symantec gekauft wurde. Nach allen bisherigen Erfahrungen werden die auch die Programme von Sysinternals eklatant "verbessern" 

Ich dachte eigentlich das Microsoft der Käufer war.

Beitrag von „Hagen“ vom 8. August 2006 um 17:47

Wie auch immer. Die Beta ist fürchterlich langsam. Zumindest auf einer virtuellen Maschine.

Hat sich schon mal jmd. das neue Office angesehen? Otto Normalverbraucher wird sich über die Oberflächenänderungen bestimmt freuen...

Beitrag von „darkdiver“ vom 8. August 2006 um 18:06

Ich habe das VISTA und das Office auf einer realen Maschine laufen. Vista ist schneller als ein frisch installiertes XP und Office mit seinem neuen Userinterface macht Sinn.

Sicherlich wird es eine Umstellung geben, aber das ist Microsoft sicherlich bekannt, nur sind die Anpassungen rein ergonomisch und somit sehr intuitiv.

Ich kann Microsoft nur gratulieren, diesen Schritt im Office gemacht zu haben.

Viele Grüße
Eric

Beitrag von „jome“ vom 8. August 2006 um 22:39

> Zitat von Hagen

> Ich dachte eigentlich das Microsoft der Käufer war.

da hast Du Recht und mein Info-Dienst mich ganz schön verladen. 

Allerdings ändert dies an der weiteren Aussage nur wenig.