Link: https://www.computerwoche.de/a/neue-attacke-ohne-doppelklick,1889406

Immer noch kein Patch für Acrobat Reader

Neue Attacke ohne Doppelklick

Datum: 09.03.2009
Autor(en): Uli Ries

Erst am 11. März will Adobe die seit Januar bekannte Lücke im extrem weit verbreiteten Acrobat Reader schließen. Jetzt ist eine neue Attacke aufgetaucht, die PCs infiziert, ohne dass der Anwender das infizierte PDF öffnen muss. Selbst ein einzelner Klick oder das Ruhen des Mauszeigers auf dem Dokument genügt.

Laut Antiviren-Experten wie **Symantec**[1] wird die von **Adobe**[2] bestätigte und in sämtlichen Versionen des Acrobat Readers **existierende Lücke**[3] bereits seit Anfang Januar aktiv ausgenutzt. **Betroffen**[4] sind sowohl Windows- als auch Mac-OS-X-Systeme. Jetzt hat der Sicherheitsexperte Didier Stevens eine neue Variante der Attacke **veröffentlicht**[5], die zwar nicht unter Mac OS X funktioniert, dafür aber ohne weiteres Zutun des Anwenders zur Infektion von Windows-PCs mit Malware führt.

Wie ein Videoclip in Stevens' Weblog belegt, wird die Lücke in den Acrobat-Reader-Komponenten auch dann zum Sicherheitsproblem, wenn ein Anwender die mit Malware verseuchte PDF-Datei im Windows Explorer lediglich einmal anklickt oder gar nur den Mauszeiger über der Datei ruhen lässt. Und selbst die simple Anzeige des Ordners, in der die Datei liegt, ist eine Gefahr. Zumindest dann, wenn die „Miniaturansicht" im Explorer gewählt wurde. In all diesen Fällen ruft der Explorer automatisch die von Acrobat Reader mit installierte Windows-Explorer-Shell-Erweiterung auf. Die Erweiterung nutzt Funktionen der DLL, in der die Sicherheitslücke entdeckt wurde. Sicherheitsexperte Stevens gibt an, dass seine Proof-of-Concept-Attacken auf einem vollständig gepatchten Windows XP SP2 funktionieren. Er geht jedoch davon aus, dass auch andere Windows-Varianten angreifbar sind.

Auch die Suchfunktion von Windows kann den Schadcode aktivieren: Der von der Windows-Suche benötigte Windows-Index-Service greift beim Erstellen des Index ebenfalls auf die fehlerhafte Adobe-DLL zurück. Zumindest unter Windows XP Service Pack 2 ist der Indexdienst aber nicht standardmäßig aktiviert.
Um die neuen Attacken von Didier Stevens abzuwehren, genügt es nicht mehr, JavaScript im Acrobat Reader abzuschalten. Dies ist ein wirksames Mittel gegen die bislang kursierenden Attacken. Stevens hingegen nutzt JavaScript nicht. Daher bleibt IT-Verantwortlichen nur, die Shell Extension zu deaktivieren. Hierzu bieten sich die Freeware-Tools **ShellExView**[6] von Nirsoft oder Microsoft **Autoruns**[7].

Angesichts der neuartigen, weiter verfeinerten Angriffsmethoden sollten Administratoren den für 11. März versprochenen Acrobat-Reader-Patch umgehend testen und auf alle PCs im Unternehmen zu verteilen.

Links im Artikel:

[1] **http://www.symantec.de/**
[2] **https://www.computerwoche.de/knowledge_center/office_tools/1873993/**
[3] **http://www.adobe.com/support/security/advisories/apsa09-01.html**
[4] **https://www.computerwoche.de/knowledge_center/security/1888142/**

[5] **http://blog.didierstevens.com/2009/03/04/quickpost-jbig2decode-trigger-trio/**

[6] **http://www.nirsoft.net/utils/shexview.html**

[7] **http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx**

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.