Sicherheitslücke in Safari demonstriert

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Die Mac-Sicherheitsexperten Dino Dai Zovi und Charlie Miller haben am gestrigen Mittwoch auf der vom Dienstleister cirosec veranstalteten Sicherheitskonferenz IT-Defense 2011 einen Zero-Day-Exploit für das 64-bittige Safari 5 gezeigt. Dabei übernahm Miller auf einem mit allen Sicherheitsupdates ausgestatteten MacBook mit einem simplen URL-Aufruf die Kontrolle über den Safari-Prozess. Mit Details wollten die beiden Experten zwar nicht herausrücken, da der Exploit möglicherweise auch auf dem Anfang März stattfindenden Wettbewerb Pwn2Own gewinnbringend zum Einsatz kommen soll.

Die Demonstration zeigte aber wieder einmal, wie verwundbar Apples Betriebssystem und Anwendungen trotz Sicherheitsmaßnahmen wie Address Space Layout Randomization (ASLR) und Data Execution Prevention (DEP) sind: Mac-Anwender dürfen sich aufgrund mangelnden Engagements der Malware-Produzenten zwar bislang sicher fühlen, gezielten Angriffen hält Snow Leopard jedoch nicht stand. Sicherheitsexperten halten OS X daher durchweg für deutlich unsicherer als Windows 7 (mehr dazu in c't 4/2011, "Security paradox").

Die zwei US-Amerikaner gehen sogar noch einen Schritt weiter. Einige Sicherheitsgewinne in Snow Leopard bezeichneten sie als "Zufallsprodukte". So lässt Apples Implementierung der ASLR mit diversen festen Einstiegsadressen weiterhin zahlreiche Türen offen. DEP ist zwar für 64-Bit-Prozesse vernünftig implementiert, JIT-Spraying (zugehöriges White Paper) ist aber in der Lage, ASLR plus DEP auszuhebeln. Da etwa Safari auf WebKit beruht, funktioniert der Angriff dennoch nicht: WebKit randomisiert nämlich die Speicheradresse des produzierten JIT-Codes eigenhändig; da hat das WebKit-Projekt wohl Apple nicht getraut.

Ebenso haben mit OS X 10.6 eingeführte Änderungen in der Speicher-verwaltung – malloc stellt Speicher nun je CPU-Kern in einer Magazin genannten Zone bereit – Sicherheitsvorteile, die so ursprünglich wohl nicht eingeplant waren. Miller klassifiziert die Änderungen als "Performance-Verbesserungen". Die Sicherheitsproblematik bei Apple beleuchtet Mac & i intensiv in der Erstausgabe, in der auch ein ausführliches Interview mit Dai Zovi und Miller erscheint. Das Heft ist ab 26. Februar im Handel erhältlich.

Auch die von Jeremiah Grossman präsentierte und von einem Experten-Gremium gekürte Top-10-Aufstellung der fiesesten Web-Hacking-Angriffs-techniken des Jahres 2010 enthält eine bittere Pille für Apple-Anwender. Neben dem famosen Evercookie bedroht nämlich ausgerechnet eine durch Cross-Site-Scripting ausnutzbare Schwachstelle von Safaris AutoComplete-Feature den Anwender: Injiziertes JavaScript entlockt dem Browser innerhalb weniger Sekunden durch stures Ausprobieren die zu einem früheren Zeitpunkt eingegeben Daten aus Formularfeldern. Da dies auch für den Passwort-Manager gilt, sind Anwender gut beraten, ein externes Tool wie 1Password zu verwenden.

heise.de 10.02.11