Sicherheitslücken in Microsoft-Produkten

Microsoft warnt vor einer kritischen Sicherheitslücke im DirectShow-Filter Quartz.dll der DirectShow-Bibliothek zum Abspielen von QuickTime-Videos. Angreifer nutzen die Lücke bereits aktiv aus. Dazu genügt es, dass ein Opfer eine Webseite mit einem präparierten Video besucht, um ohne weitere Interaktion einen Trojaner untergeschoben zu bekommen. Dabei spielt es keine Rolle, mit welchem Browser man die Seite aufruft. Betroffen sind nur Windows 2000, XP und Server 2003 mit DirectX 9 (a,b,c). Bis Redaktionsschluss arbeiteten die Redmonder noch an einem Patch. Bis zur Veröffentlichung soll es helfen, einen Registry-Schlüssel zu löschen, um das Laden des verwundbaren Filters zu verhindern.

Eine Anleitung dafür findet sich im „Security Research & Defense"-Blog (siehe Webcode).

Zudem hat Microsoft eine Lücke im Internet Information Server 5.0, 5.1 und 6.0 bestätigt. Durch einen Fehler in der WebDAV-Funktion beim Dekodieren von URLs mit Unicode ist es möglich, die Authentifizierungsfunktionen auszuhebeln und auf geschützte Daten zuzugreifen. Einen Patch gibt es ebenfalls noch nicht. Bis zu dessen Erscheinen schlägt Microsoft zwei Workarounds vor: WebDAV abschalten oder Zugriffe des anonymen Nutzers blockieren. Anleitungen dafür hält Microsoft in seinem Fehlerbericht bereit (siehe Webcode). **(dab)**

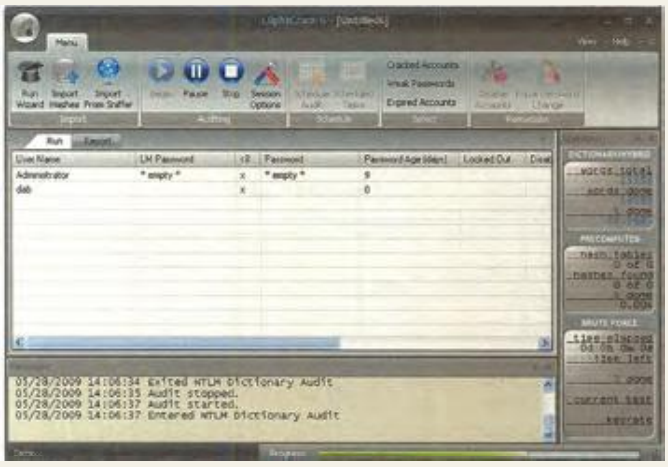
www.dmagazin.cle/0913048

Tools und Produkte

Im Rahmen seines **Security Development Lifecycle** (SDL) hat Microsoft ein Tool zum Download bereitgestellt, mit dem Programmierer das gesammelte Wissen des SDL in die eigene Softwareentwicklungsumgebung integrieren können. SDL ist Microsofts Prozess, um möglichst sichere und fehlerfreie Software herzustellen. Das Tool beruht auf einem Process Template für Visual Studio Team System.

Secunias **Personal Software Inspektor** (P51) bringt in der aktuellen Beta-Version die Option „Sicheres Browsing" mit. Sie warnt vor dem Einsatz eines Browsers, wenn gefundene Plugins und Add-ons unsicher sind.

Das ehemalige LOphtcrack-Team hat Anfang des Jahres die Rechte an seinem legendären Tool von Symantec zurückgekauft und es weiterentwickelt. **LOphtCrack 6** läuft nun auch auf 64-BitVersionerr von Windows und unterstützt Mehrkernsysteme sowie vorberechnete Hash-Tabellen (Rainbow-Tables), um Windows- und Unix-Passwörter zu knacken beziehungsweise um „ihre Stärke zu testen". Die Tests lassen sich lokal und über das Netzwerk in regelmäßigen Abständen automatisch durchführen. Die günstigste Variante soll knapp 300 US-Dollar kosten, eine Trial-Version für 14 Tage steht ebenfalls bereit. **(dab)**



Viel hat sich in der Bedienoberfläche von LOphtCrack 6 im Vergleich zur Vorgängerversion nicht getan.

iTAN-Verfahren keine Hürde mehr

Das iTAN-Verfahren hindert laut BKA Kriminelle nicht mehr daran, Konten von Bankkunden leer zu räumen. Die indizierten Transaktionsnummern waren eingeführt worden, nachdem sich das herkömmliche TAN-System gegenüber Phishing-Attacken als zu unsicher gezeigt hatte. Zwar seien Phishing-Angriffe mit iTAN schwieriger geworden, aber nicht unmöglich.

Bereits Ende 2005 hatte eine Arbeitsgruppe der Ruhr-Universität Bochum einen Angriff auf das Online-Banking-Verfahren mit indizierten TANs erfolgreich demonstriert. Anfang 2007 tauchten dann erste Phishing-Kits auf, die in der Lage waren, per Man-in-the-Middle-Attacke abgephishte iTANs in Echtzeit für eigene Transaktionen zu benutzen. Auch heise Security erreichen immer öfter Meldungen von Lesern über Trojaner-basierte Phishing-Angriffe, die trotz iTAN-Verfahren erfolgreich waren. Als sehr sichere Verfahren gelten derzeit mTAN beziehungsweise SMS-TAN und Chipkartenverfahren wie HBCI und Secoder. **(dab)**

Exploit für Mac OS X

Der Sicherheitsspezialist Landon Fuller hat einen Exploit für Mac OS X veröffentlicht, durch den Angreifer die Kontrolle über einen Rechner übernehmen könnten. Dazu muss ein Anwender lediglich mit einem Browser eine manipulierte Webseite aufrufen. Ursache der Drive-by-Download-Lücke sind seit Anfang Dezember bekannte Schwachstellen der Sandbox der Java Virtual Machine bei der Deserialisierung bestimmter Objekte. Damit kann ein (untrusted) Applet an höhere Systemrechte gelangen. Die Demo startet indes nur eine harmlose Sprachausgabe.

Sun hat die Lücken bereits unter anderem mit Java 6 Update 11 im Dezember geschlossen — bei Apple ist dies bislang nicht der Fall. Abhilfe bringt derzeit nur, im jeweiligen Browser Java zu deaktivieren, bei Safari beispielsweise unter „Safari/Einstellungen/Sicherheit". **(dab)**

Sicherheitsnotizen

In der quelloffenen Implementierung des Network Time Protocol **ntpd** steckt ein Fehler, durch den Angreifer aus der Ferne ein System zum Absturz bringen oder kompromittieren können. Ein Patch korrigiert den Fehler.

Präparierte PDF-Dateien können nach Angaben des **BlackBerry**-Herstellers RIM dazu führen, dass ein Angreifer einen BlackBerry-Server unter seine Kontrolle bringt. Updates schließen die Lücke.

Angreifer können Schwachstellen im Solaris-Dienst sadmind ausnutzen, um aus der Ferne Befehle mit Root-Rechten auszuführen. Der Hersteller Sun hat Patches für Solaris 8 und 9 bereitgestellt.

Novell hat Updates für **GroupWise** 7.x und 8.x veröffentlicht, die sechs Sicherheitslücken schließen sollen. Zwei der Lücken beruhen auf Buffer Overflows im GroupWise Internet Agent, die sich aus der Ferne ausnutzen lassen.

In Version 1.0.8 des Netzwerkanalysators **Wireshark** haben die Entwickler unter anderem eine DoS-Schwachstelle beim Verarbeiten des PCNFSD-Protokolls beseitigt.

Adobe will ab kommendem Sommer einen regelmäßigen Patch-Zyklus für **Adobe Reader** und **Acrobat** einführen. Alle drei Monate sollen parallel zum Microsoft-Patchday am zweiten Dienstag eines Monats Sicherheits-Updates erscheinen.

Die Entwickler des Instant-Messaging-Clients **Pidgin** haben in Version 2.5.6 mehrere Sicherheitsprobleme gelöst.