Forscher knacken digitale PDF-Signatur Sicherheitsstandard für Dokumente umgehbar - Nur Update auf neuester Adobe-Version schützt

Forscher der Ruhr-Universität Bochum haben schwere Sicherheitslücken bei PDF-Signaturen entdeckt. So lassen sich Dokumente manipulieren, ohne dass die Signatur dadurch ungültig wird. "Unsere Vorbereitung auf diese Angriffe war sehr aufwendig, doch wenn man weiss, was man tun muss, kann man die Signatur binnen weniger Minuten umgehen", sagen die Forscher Vladislav Mladenov und Christian Mainka im Gespräch mit pressetext.
Digitale Signaturen sollen anzeigen, ob jemand auf ein Dokument zugegriffen oder es verändert hat. Dadurch wird gewährleistet, dass ein PDF vom angegebenen Absender stammt. Seit 2014 in der EU die Regulierung zu "Electronic Identification, Authentication and Trust Services" in Kraft getreten ist, sind digitale Signaturen in vielen Bereichen zu finden. Auch Unternehmen benutzen sie für Rechnungen, in Ã–sterreich werden sie sogar für Gesetzesdokumente verwendet.

Inhalt beliebig veränderbar

In der Untersuchung wurden 22 gängige Desktop-Applikationen für Windows, Linux und MacOS sowie weitere sieben Online-Services analysiert. Bei letzteren handelt es sich um Webseiten, deren Aufgabe es ist, die Signatur eines hochgeladenen PDF-Dokuments zu überprüfen. Sie werden zum Beispiel von Behörden und Unternehmen verwendet. 21 der getesteten Desktop-Anwendungen und fünf der Online-Services waren verwundbar. Durch unterschiedliche Arten von Angriffen konnten die Forscher PDF-Dokumente beliebig manipulieren. So verwandelten sie beispielsweise einen zu zahlenden Rechnungsbetrag in eine Kostenrückerstattung von einer Bio. Dollar, ohne die Signatur der PDF-Rechnung zu kompromittieren.

"Wir haben verschiedene Varianten von Angriffen verwendet, zum Beispiel haben wir beim Universal Signature-Forgery-Ansatz Informationen im Signaturobjekt verändert. Dadurch waren Signaturdaten nicht vorhanden, Adobe hat aber fälschlicherweise angenommen, dass die Signatur unverändert geblieben ist. Ein anderer Ansatz war die Incremental Saving Attack. Es gibt bei PDFs die Möglichkeit, das Dokument beliebig zu erweitern, wie beispielsweise durch Kommentare, was die Spezifikation erlaubt. Wir haben ganze Dokumente angefügt und den vorherigen Inhalt ausgeblendet, so entsteht ein völlig neues Dokument, ohne dass die Anwendung das merkt", meinen Mladenov und Mainka.

Durch Updates schützen

Doch es gibt einen Schutz, so Mladenov und Mainka: "Unsere Lösung dafür ist, die PDF Viewer auf die neueste Version upzudaten. Es ist ratsam, immer auf der letzten Version von Adobe Acrobat zu sein. Es ist natürlich nicht auszuschliessen, dass dieses Problem in Zukunft wieder auftreten könnte, aber momentan funktioniert diese Lösung. Es ist wichtig, künftige Schwachstellen sofort zu melden. Wenn man diese Sicherheitslücken adressiert und löst, spricht nichts dagegen, weiter PDFs zu verwenden. Es ist uns auch momentan nicht bekannt, dass schon jemand diese Manipulation in die Tat umgesetzt hat. Wer auch immer auf PDFs angewiesen ist, ob für Rechnungen oder vertrauliche Dokumente, muss aber unbedingt die Software aktualisieren."