Hash-Verfahren SHA-1 am Ende

Das Hash-Verfahren SHA-1 gilt seit langem als unsicher; Forscher von Google und dem Forschungsinstitut CWI Amsterdam belegten das mit ihrem SHAttered-Angriff nun auch in der Praxis: Sie erstellen zwei PDF-Dokumente mit unterschiedlichem Inhalt, welche den gleichen SHA-1-Hash-Wert ergeben. Mehr als 6500 CPU-Jahre und noch mal 100 GPU-Jahre erforderte die Berechnung dieser Kollision.

Hash-Verfahren wie SHA-1 und dessen Nachfolger SHA-2 kommen immer dann zum Einsatz, wenn es darum geht, eine kompakte Darstellung großer Datenmengen zu finden, um deren Echtheit zu bestätigen. Also etwa bei digitalen Signaturen von Programmen, Updates, Krypto-Schlüsseln, Backups oder E-Mails. Die wichtigste Anforderung ist: Jede noch so kleine Änderung des Datensatzes führt zugleich zu einer Änderung des Hash-Wertes. Darüber hinaus muss es auch praktisch unmöglich sein, dass jemand zwei Datensätze erstellt, die den gleichen Hash-Wert produzieren. Genau das gewährleistet SHA-1 definitiv nicht mehr.

Mancher mag denken, dass die benötigte Rechenzeit die Latte immer noch ausreichend hoch hängt. Doch angesichts von Cloud Computing und dem immer noch gültigen Moore'schen Gesetz zum Wachstum der Rechenleistung kombiniert mit weiteren Fortschritten bei den Angriffen ist das ein gefährlicher Irrtum. So mussten etwa 2008 die Forscher um Marc Stevens noch einen Cluster von über 200 Playstation-3-Konsolen mehrere Tage für eine MD5-Kollision rechnen lassen. Heute schafft das jeder PC in weniger als einer Sekunde.

SHA-1 gilt bereits seit 2005 als geknackt. Damals stellten chinesische Kryptologen einen Angriff vor, der die Zahl der benötigten Berechnungen für das Auffinden einer Kollision deutlich reduzierte. Dieser war zwar immer noch weit von einer praktischen Realisierbarkeit entfernt. Nach dem jetzt von Marc Stevens und Kollegen vorgestellten Angriff auf SHA-1 kann man dieses Hash-Verfahren aber endgültig beerdigen; wer es jetzt noch einsetzt, handelt grob fahrlässig. Der Nachfolger steht auch schon fest: In allen praktischen Belangen kann und sollte man stattdessen SHA256 oder SHA512 verwenden. Diese beiden SHA-2-Varianten gelten als ausreichend sicher; Alternativen sind SHA-3 und Blake. *(ju@ct.de)*

Weitere Hintergründe zum SHA-1-Angriff: ct.de/ynvh

Erfolgreicher Angriff auf SHA-1: Bei der linken PDF-Datei ist der Hintergrund blau, rechts ist er rot – trotzdem kommt die gleiche SHA-1-Prüfsumme heraus.

Patch-Chaos bei Microsoft

Im Februar ließ Microsoft erstmals seinen Patchday ausfallen. Das Unternehmen erklärte kurz vor dem traditionellen Veröffentlichungstermin am zweiten Dienstag des Monats, dass man in letzter Minute auf ein Problem gestoßen sei. Die vorenthaltenen Patches für Windows & Co. sollen am 14. März erscheinen – also am regulären März-Patchday, der entsprechend umfangreicher ausfallen dürfte.

Unterdessen verschärfte sich die Situation für Windows-Nutzer durch zwei ungepatchte Schwachstellen (sogenannte Zero-Day-Lücken), welche das Google-Sicherheitsteam Project Zero öffentlich gemacht hat. Eine davon klafft in der Grafikbibliothek GDI des Windows-Kernels, die andere in Internet Explorer und Edge. Letztere Lücke kann ein Angreifer offenbar zum Einschleusen von Schadcode missbrauchen. In beiden Fällen hatte Microsoft vor der Bekanntmachung durch Google drei Monate Zeit, zu patchen. Nach wie vor klafft zudem die seit Anfang Februar bekannte Denial-of-Service-Lücke in der SMB-Bibliothek von Windows. Angreifer können sie ausnutzen, um Windows-Clients und -Server zum Absturz zu bringen.

(rei@ct.de)

Details zu den Zero-Day-Lücken: ct.de/ynvh

Erpressungs-Trojaner wohnt im UEFI

Auf der RSA Conference in San Francisco demonstrierten Sicherheitsforscher die Gefahren des Unified Extensible Firmware Interface (UEFI) anhand eines besonders perfiden Erpressungs-Trojaners: Der zu Anschauungszwecken entwickelte Schädling nistet sich in das UEFI ein, um den Start des Rechners zu blockieren und eine Erpresser-Botschaft anzuzeigen. Nicht mal an die UEFI-Einstellungen kommt man mehr heran. Die Forscher infizierten ein Gigabyte-Mainboard (Intel Skylake), es sollen jedoch auch Mainboards anderer Hersteller angreifbar sein.

Der zur Demonstration verwendete Computer lief den Sicherheitsforschern zufolge mit einem vollständig gepatchten Windows 10 – die Schutzmechanismen Device Guard, Secure Boot und Virtual Secure Mode sollen ebenfalls aktiv gewesen sein. In der Live-Demo begann die Infektion mit einem präparierten Word-Dokument, das per Makros und Powershell einen Dropper herunterlud. Dieser wiederum zog den BIOS-Updater des Mainboard-Herstellers aus dem Netz und installierte ihn. An dieser Stelle wäre es in der Realität aber knifflig geworden, da ein potenzielles Opfer die Installation des Updaters bestätigen muss.

Mit nicht näher genannten Exploits umgingen die Sicherheitsforscher den Schreibschutz des Flash-Speichers und konnten so ihre um die Ransomware erweiterte Variante der Firmware auf das Mainboard flashen. Das funktionierte, weil der Update-Prozess die Firmware laut den Forschern nicht auf Integrität überprüft, keine der Komponenten sei digital signiert.

(Uli Ries/des@ct.de)