Microsoft schließt die LNK-Lücke – erneut

An seinem Patchday im März hat Microsoft 54 Sicherheitslücken mit insgesamt 14 Sammel-Updates geschlossen. Für Aufmerksamkeit sorgte vor allem ein Patch für die sogenannte LNK-Lücke, die Microsoft eigentlich schon 2010 geschlossen hatte. Wie ein deutscher Student entdeckte, war der damalige Fix allerdings nicht umfassend genug und konnte nach wie vor umgangen werden, sodass Microsoft nun noch einmal einen Patch nachlegen musste. Die LNK-Lücke erreichte unter anderem damit Bekanntheit, dass der Stuxnet-Wurm sie für seine Verbreitung nutzte.

Ein Patch für Windows 7 und Server 2008 R2, der im Oktober 2014 erst veröffentlicht und dann nach Kompatibilitätsproblemen wieder zurückgezogen worden war, wurde ebenfalls neu verteilt. Das blieb auch dieses Mal nicht ganz ohne Nebenwirkungen, da das Update auf manchen Systemen, die neben Windows auch Linux installiert hatten, Boot-Probleme verursachte. Wenn Windows und Linux auf zwei unterschiedlichen Platten lagen und mit klassischem BIOS gebootet wurde, konnte es passieren, dass Windows in einer Schleife hängen blieb. UEFI-Systeme waren nicht betroffen.

Neben alten hat Microsoft aber auch neue Probleme behoben: Unter anderem wurde die Freak-Schwachstelle in der Windows-Kryptoinfrastruktur SChannel abgedichtet. Ein Sammel-Update für den Internet Explorer schloss ebenfalls eine große Zahl von Sicherheitslücken. (fab@ct.de)

Das SecuTablet dient als Pendant zu den verschlüsselnden Smartphones der Düsseldorfer BlackBerry-Tochter SecuSmart.

IBM und SecuSmart stellen sicheres Tablet vor

Die deutsche BlackBerry-Tochter SecuSmart hat auf der CeBIT zusammen mit IBM ein verschlüsseltes Tablet vorgestellt. Das SecuTablet ist, ähnlich wie die verschlüsselnden Smartphones der Firma, für den Einsatz in Behörden und Firmen gedacht und basiert auf dem Samsung Tab S 10.5 – es soll als Begleiter für die BlackBerry-Handys dienen. Private und geschäftliche Apps laufen auf dem Gerät in getrennten Zonen. So können private Programme wie Facebook, Twitter und WhatsApp vertrauliche Daten nicht in Mitleidenschaft ziehen.

IBM stellt Virtualisierungstechnik zur Verfügung, die bei der Absicherung von Apps auf dem Tablet zum Einsatz kommt, und bietet Servertechnologie, die Großkunden bei der Verwaltung der Tablets unterstützen soll. Das SecuTablet wird momentan vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft. Es soll nach Abschluss der Prüfung die Zulassung für die niedrigste Geheimhaltungsstufe „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) erhalten. (fab@ct.de)

Finanzkrise bei GnuPG abgewendet

Nach einer Welle an Spenden sieht GnuPG-Entwickler Werner Koch zuversichtlich in die Zukunft: „Die finanzielle Krise des GnuPG-Projektes ist vorbei“, schrieb er in einem Blog-Eintrag. Nach Medienberichten über die Finanzmisere (siehe c’t 5/15, S. 38) gingen über 180 000 Euro bei dem Projekt ein und Facebook sowie der Bezahldienst Stripe sicherten jährliche Zahlungen zu. Jetzt könne man einen zweiten Entwickler einstellen, so Koch.

GnuPG setzt den PGP-Standard um und ist eins der wichtigsten quelloffenen Kryptosysteme. Es wird von Nutzern weltweit eingesetzt, um E-Mails zu verschlüsseln. Lange Zeit hatte Koch die Software im Alleingang entwickelt – eine Aufgabe, mit der er sich eher schlecht als recht hatte über Wasser halten können. (fab@ct.de)

Rowhammer: Root-Rechte durch Speichermanipulationen

Forscher von Googles Project Zero haben es geschafft, auf aktuellen DRAM-Chips mit Absicht sogenannte Bit Flips auszulösen und sich damit Root-Rechte zu verschaffen. Damit haben sie aus einem Zuverlässigkeits-Problem eine Sicherheitslücke gemacht. Um das zu untermauern, veröffentlichten sie entsprechenden Testcode. Dass auf solchen Chips unter bestimmten Umständen Lese-Operationen dazu führen, dass in benachbarten Speicherbereichen Daten verändert werden, war der Industrie bereits bekannt – die Ergebnisse der Google-Forscher bauen auf einer entsprechenden Studie ihrer Kollegen der Carnegie-Mellon-Universität und der Intel Labs auf. Bis jetzt hatten Speicherhersteller dieses Phänomen allerdings eher als Qualitätsdefizit der Hardware gesehen. Die Google-Forscher beweisen nun, dass es sich auch für konkrete Angriffe auf Rechner missbrauchen lässt.

Bei dem als „Rowhammer“ bezeichneten Angriff greifen die Forscher immer wieder auf einen bestimmten physischen Bereich des Speichers zu und schaffen es so unter Umständen, Bits in einem angrenzenden Bereich zu flippen: Aus Einsen werden dann Nullen oder umgekehrt. Damit lässt sich mit Nutzerrechten ein Speicherbereich manipulieren, der einem Prozess gehört, der mit Administratorrechten läuft. Nach eigenen Angaben schafften sie es so, aus der NaCl-Sandbox des Chrome-Browsers auszubrechen. Auch auf Linux lassen sich so Root-Rechte erschwindeln. Prinzipiell ist aber jedes Betriebssystem auf diese Art angreifbar, bei konkreten Angriffen auf Notebooks stellten sich allerdings Modelle von bestimmten Herstellern als empfindlicher heraus als andere. Allerdings behielten die Forscher für sich, welche Geräte verwundbar sind und welche nicht. ECC-RAM, wie es vor allen bei Servern zum Einsatz kommt, scheint den Angriff zu vereiteln. (fab@ct.de)

Sicherheits-Notizen

In Version 4.1.00 des Online-Shop-Systems **xt:Commerce** klafft eine schwerwiegende Sicherheitslücke. Der Anbieter rät Nutzern zu einem Update auf die Versionen 4.1.10 oder 4.2.00.

Google hat versehentlich die Identitäten von fast 300 000 Domain-Inhabern bekannt gegeben, die eigentlich mit einem anonymen WHOIS-Eintrag registriert wurden. Nach Mitte 2013 hatte Google die Anonymisierungsfunktion nach und nach abgeschaltet, was die E-Mail-Adressen und Telefonnummern der Kunden offengelegt hatte.

Adobe hat mit einem Sprung auf Version 17 mehrere Sicherheitslücken im **Flash Player** gestopft. Updates, auch für ältere Flash-Ausgaben, stehen für Windows, OS X und Linux bereit.