Streit mit Google: Symantec knickt ein

Seit Symantec 2015 mit einem gefälschten Google-Zertifikat erwischt wurde, schwelt der Streit zwischen den Unternehmen. Es geht darum, ob Google weiter zu Symantec gehörende CAs wie Thawte oder Verisign in seinen Browser integriert. Google hatte Symantec mit einem Ultimatum gezwungen, seinem Certificate-Transparency-Programm beizutreten. Bei Certificate-Transparency müssen CAs alle Zertifikate in einen Hash-Baum eintragen, wodurch entweder Manipulationen oder gefälschte Zertifikate für immer sichtbar bleiben. Auf Basis der Daten wirft Google Symantecs Zertifizierungsstellen vor, 30.000 Zertifikate nicht korrekt ausgestellt zu haben. Symantec weist diesen Vorwurf zurück und will „das Missverständnis“ klären. Damit Chrome ihre Zertifikate weiter als vertrauenswürdig anzeigt, hat Symantec nun angekündigt, sie künftig von Dritten prüfen zu lassen. Ein bisher nicht benannter externer Dienstleister soll bis 31. August alle Extended-Validation-Zertifikate prüfen. Zusätzlich soll es Prüfungen aktiver Zertifikate von Partnern wie CrossCert geben.

Außerdem geht Symantec auf Googles Forderung ein, regelmäßiger neue Zertifikate auszustellen. Ab Ende August will die CA SSL-/TLS-Zertifikate anbieten, die nur drei Monate lang gültig sind. Bei der Verlängerung von Zertifikaten, die länger als neun Monate gültig waren, will Symantec eine kostenlose Domain-Validierung einführen. Kommende Chrome-Versionen sollen neu ausgestellten Zertifikaten nämlich nur noch für neun Monate und weniger vertrauen.

(des@ct.de)

Häufigere Updates für Windows 10

Microsoft will ab dem Creators Update auch außerhalb des Patchdays per kumulativem Update neue Funktionen für Windows 10 ausliefern. Routinemäßig soll ein zusätzliches Update im Monat ausgespielt werden, manchmal auch mehr.

Der Patchday war bislang ein Zugeständnis an Admins, damit die jeden Monat einen festen Tag zum Updaten einplanen können. Die Microsoft-Entwickler tragen sich jedoch schon seit Jahren mit dem Gedanken, den Patchday abzuschaffen oder wenigstens stark aufzuweichen. Microsoft möchte selbst entscheiden, wann welche Updates installiert werden.

Seltsamerweise schließt Microsoft Sicherheits-Updates komplett von dieser Praxis aus. Die Gründe dafür erklärt die Ankündigung im Microsoft-Blog leider nicht. Sicherheitsforscher drängen den Windows-Hersteller seit Jahren dazu, außer der Reihe zu patchen. Sie beklagen, dass Microsoft kriminellen Hackern mit voller Absicht ein Handlungsfenster von fast einem Monat gewährt, falls diese eine Zeroday-Lücke direkt nach einem Patchday angreifen. Man opfere damit die Sicherheit von Millionen Endnutzern zugunsten gut zahlender Geschäftskunden.

(fab@ct.de)

Firmware-Lücke in Intel-Systemen

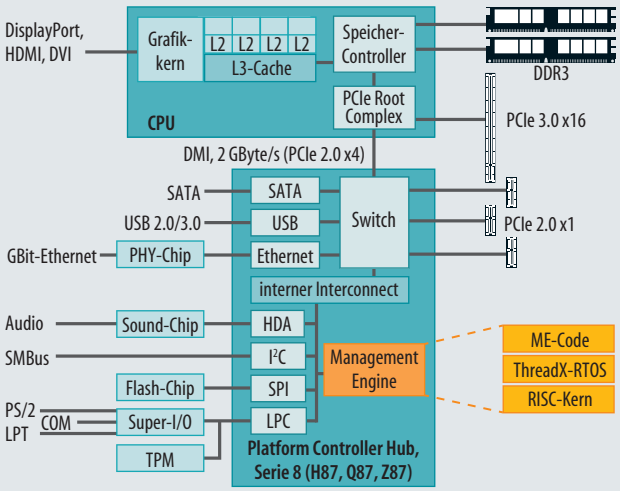
Die Firmware von Intels oft kritisierter Management Engine (ME) enthält eine Sicherheitslücke, über die Angreifer via Netzwerk höhere Zugriffsrechte erlangen können. Die ME ist ein zusätzlicher Mikrocontroller, der seit 2010 in fast allen PCs, Notebooks und Servern mit Intel-Prozessoren sitzt und dessen Firmware Zugriff auf RAM und Netzwerk hat. Die ME-Firmware kann in verschiedene Betriebsmodi schalten; angreifbar sind nur die Active Management Technology (AMT), Intel Standard Manageability (ISM) und Small Business Advantage (SBA). Die Lücke betrifft daher Systeme mit Core-i-Prozessoren und ME-Fernwartungsfunktionen sowie mit dem Core i verwandte Xeons, Pentiums und Celerons.

Intel hat bereits Updates der ME-Firmware für alle betroffenen Systeme bereitgestellt. Diese Updates können PC- und Mainboard-Hersteller in ihre BIOS-Updates für die betroffenen Systeme integrieren. Bisher liegen uns jedoch keine Informationen über solche BIOS-Updates vor. Die ME-Firmware lässt sich bei vielen Systemen auch unabhängig vom BIOS-Code patchen. Aber auch dann sollte der Systemhersteller ein passendes Update bereitstellen. Pikanterweise hat bislang nicht mal Intel selbst für seinen NUC5i5MYBE mit vPRO-Fernwartungsfunktion ein Update veröffentlicht.

Die Management Engine steckt in Desktop-PCs und Notebooks mit besonderen Intel-Netzwerkchips (Ethernet und WLAN) für Fernzugriff auf BIOS-Setup und grafischen Desktop (Remote KVM). Intel vermarktet diese Systeme als vPRO-Bürocomputer. Auch „U“-Mobilprozessoren in teuren Business-Notebooks sind betroffen. Die Verwundbarkeit prüft man mit dem Intel SDS – System Discovery Utility, das Funktionstyp und Firmware-Version der ME ausliest. Bei unsicheren Systemen meldet das Programm eine Build-Nummer unter 3000. *(ciw@ct.de)*

Management Engine im Intel-Chipsatz

Über Lücken in der ME könnten Angreifer beispielsweise Passwörter aus dem RAM lesen, ohne dass das Betriebssystem etwas dagegen tun kann.



Bankkonten über UMTS-Lücke ausgeräumt

Über Phishing erbeuten Kriminelle relativ leicht Zugangsdaten für das Online-Banking zahlreicher deutscher Bankkunden. Um an Mobil-TANs (mTANs) für Überweisungen zu kommen, mussten sie aber bisher immer Trojaner auf die Mobilgeräte der Opfer schleusen oder deren SIM-Karten klonen lassen. Dank einer seit Jahren bekannten Sicherheitslücke im UMTS-Netz konnten sie sich diesen Aufwand jetzt sparen. Mit der Lücke im SS7-Protokoll leiteten die Angreifer SMS-Nachrichten mit mTANs um und empfingen sie auf eigenen Geräten. Damit die Opfer von der Umleitung nichts mitbekamen, fanden die Angriffe wohl nachts statt.

Eigentlich wollten die Provider schon 2014 Gegenmaßnahmen gegen die SS7-Lücke ergreifen. Hacker hatten die Lücke bereits auf dem 31C3 präsentiert. Im März hatten Experten erneut vor der Lücke gewarnt. O2 Deutschland bestätigte gegenüber der Süddeutschen Zeitung, dass schon im Januar dieses Jahres SS7-Angriffe im eigenen Netz stattgefunden haben. Unsere Anfrage, warum O2 die von den Experten empfohlenen Plausibilitäts-Checks nicht umgesetzt hat, beantwortete das Unternehmen bisher nicht. *(fab@ct.de)*

Sicherheits-Notizen

Cisco schließt mit einem Update mehrere Denial-of-Service-Lücken in seinen **Firewalls**.

Die Zwei-Faktor-Authentifizierung des Passwortmanagers **Lastpass** ließ sich mittels Cross-Site Request Forgery (CSRF) umgehen und sogar komplett deaktivieren. Laut Hersteller behebt ein Update die Lücke.

In der Wiki-Software **Confluence** können Angreifer seit Version 6.0.0 Page IDs durchprobieren und darüber unautorisiert Artikel einsehen. Die Updates auf die Versionen 6.0.7 und 6.1.0 beheben die Lücke.

Über eine kritische Lücke in **Drupal 8** können Angreifer aus der Ferne Informationen abgreifen, sofern das Modul RESTful Web Services aktiviert ist und die Seite Patch-Anfragen zulässt. Versionen ab 8.2.8 und 8.3.1 sowie Drupal 7 sind immun gegen den Angriff.

VMware hat mehrere kritische Lücken in **Horizon View, Unified Access Gateway** und **Workstation** geschlossen. Admins sollten unbedingt updaten, da das Notfall-Team des BSI CERT-Bund das Risiko der Lücken als „sehr hoch“ einstuft.

Die Entwickler des Continuous-Integration-Servers **Jenkins** haben in den Versionen 2.57 und 2.46.2 LTS mehrere Lücken geschlossen, mit denen Angreifer ohne Authentifizierung Schadcode auf dem Server ausführen konnten. Zudem war Jenkins für eine DoS-Attacke anfällig.