Neuer Angriff auf verschlüsselte Verbindungen

Forscher haben eine Sicherheitslücke entdeckt, mit der sich ein Teil des verschlüsselten Datenverkehrs im Internet kompromittieren lässt. Betroffen sind Verbindungen zu Web- und Mail-Servern, VPN-Verbindungen und SSH. Dem Logjam getauften Angriff liegt eine Schwäche im Diffie-Hellman-Schlüsselaustausch zugrunde. Angreifer können die geheimen Krypto-Schlüssel rekonstruieren, mit denen man gesicherte Verbindungen (zum Beispiel bei SSL/TLS) entschlüsseln und manipulieren kann. Hinter der Analyse steckt eine Reihe von Sicherheitsforschern, darunter John-Hopkins-Professor Matthew Green.

Um eine verschlüsselte Verbindung aufbauen zu können, müssen Server und Client im Vorfeld Schlüssel über eine nicht gesicherte Leitung austauschen. Dafür kommt in vielen Fällen der Diffie-Hellman-Schlüsselaustausch zum Einsatz. Dessen Sicherheit beruht darauf, dass es extrem rechenaufwendig ist, den Logarithmus großer Zahlen zu berechnen. Wie die Forscher allerdings zeigen, kann man die Rechenaufgabe so zerlegen, dass man den Großteil der Rechenarbeit schon im Vorfeld erledigen kann.

Wie viel Vorarbeit nötig ist, hängt davon ab, wie groß die verwendeten Zahlen sind. Für 512 Bit mussten die Forscher einen leistungsstarken Rechen-Cluster eine Woche arbeiten lassen. Die finale Berechnung des Logarithmus zum Knacken der Verbindung dauerte im Schnitt dann nur noch 90 Sekunden. Ab 1024 Bit ist der Aufwand erheblich größer: Nach Schätzungen der Forscher benötigt man Hardware für hunderte Millionen US-Dollar – und selbst dann würde der Rechenvorgang noch ein Jahr dauern. Dies sei aber keine Hürde für Geheimdienste wie die NSA. Ein zu Logjam passendes Diagramm aus dem Snowden-Fundus könnte sogar darauf hindeuten, dass der amerikanische Geheimdienst die Angriffstechnik bereits aktiv zum Entschlüsseln von VPN-Verkehr einsetzt.

Doch in vielen Fällen ist es gar nicht nötig, die verbreiteten 1024- oder gar 2048-Bit-Varianten von Diffie-Hellman zu knacken. Laut den Forschern bieten acht Prozent der eine Million beliebtesten Websites noch die Cipher-Suite DHE_EXPORT mit 512 Bit an. Und die meisten Browser unterstützen sie ebenfalls noch. Sie stammt aus einer Zeit, in der Krypto-Produkte in den USA noch strengen Exportbeschränkungen unterlagen. Normalerweise kommt diese Suite jedoch nicht zum Einsatz, da sich Server und Client beim Handshake stets auf die bestmögliche Verschlüsselung einigen. Den Forschern ist es allerdings gelungen, diesen Handshake als Man-in-the-Middle zu manipulieren und einem der beiden Verbindungspartner vorzugaukeln, dass sein Gegenüber lediglich DHE_EXPORT unterstützt. Anschließend nutzen beide Diffie Hellman mit 512 Bit.

Ob der eigene Browser in Gefahr ist, kann man auf der Seite der Logjam-Entdecker testen. Admins können ihre Server in einem separaten Test prüfen und finden dort auch sichere Krypto-Konfigurationen für ihre Server. Mittelfristig sollte man die Unterstützung für die Export-verkrüppelten Krypto-Verfahren endlich komplett eliminieren. Außerdem empfehlen die Forscher die Migration hin zu 2048-Bit-Diffie-Hellman und DH auf elliptischen Kurven (ECDH). (fab@ct.de/des@ct.de)

c't Schutz vor Logjam: ct.de/ywrb

Android löscht nicht richtig

Die Werks-Reset-Funktion von rund 500 Millionen Android-Geräten soll nicht zuverlässig arbeiten. Einer Studie von Forschern der Cambridge University zufolge lassen sich gelöschte Daten in vielen Fällen rekonstruieren. Bei rund 630 Millionen Android-Geräten gehen sie zudem davon aus, dass Daten von SD-Karten im Zuge des Werksresets nicht vollständig gelöscht werden. Im Zuge ihrer Untersuchung haben die Forscher unter anderem Log-in-Daten, Text-Nachrichten, E-Mails und Fotos wiederhergestellt. Eigenen Angaben zufolge haben sie das auch bei einigen Geräten geschafft, bei denen Nutzer die Vollverschlüsselung von Android aktiviert hatten, die bisher als sicher galt. Dafür mussten sie aber mehr Zeit und Mühe investieren, schließlich schützt das Nutzerpasswort oder die PIN den Schlüssel zum Dekodieren der Daten.

Für die Studie haben die Forscher 21 gebrauchte Smartphones mit den Android-Versionen 2.3.x bis 4.3 getestet. Neue Versionen sind besser vor der Entschlüsselung geschützt. Wer aus Angst um seine Daten nun eine spezielle App zum Löschen des Gerätespeichers nutzen möchte, muss aufpassen, denn oft arbeiten auch diese nicht verlässlich. Das zeigt eine weitere Studie der Forscher. (des@ct.de)

Erste-Hilfe-Kasten gegen Verschlüsselungs-Trojaner

Der Sicherheitsforscher Jada Cyrus hat eine Sammlung von Entschlüsselungs-Werkzeugen für verschiedene Cryptolocker-Trojaner zusammengestellt. Das Ransomware Response Kit enthält Entschlüsselungswerkzeuge für die Windows-Schädlinge CryptoLocker, CoinVault, FBIRansomWare und TeslaCrypt sowie das Ransomware Removal Tool von TrendMicro, welches mehrere Schädlinge entfernen kann. Zusätzlich stellt der Forscher eine Dokumentation bereit, die Opfern von Krypto-Trojanern helfen soll, solche Infektionen in Zukunft zu verhindern.

Der Forscher empfiehlt Opfern, auf die Lösegeldforderungen nie einzugehen. Stattdessen sollten sie versuchen, so genau wie möglich zu dokumentieren, welche Trojaner-Variante sie sich eingefangen haben. Dies sei wichtig, da der Einsatz des falschen Entschlüsselungs-Werkzeugs unter Umständen Daten unwiederbringlich zerstört.

Als Vorsorge sollte man regelmäßig Backups auf Platten erstellen, die ansonsten nicht an laufende Systeme angeschlossen sind. Aber auch hier ist Vorsicht geboten, da laut der von dem Forscher zusammengetragenen Dokumentation einige Schädlinge Daten heimlich im Hintergrund ver- und entschlüsseln, damit der Nutzer im Glauben gelassen wird, seine Daten und Backups sind in Ordnung. Bis der Trojaner plötzlich hinterlistig zuschlägt. Dann kann es vorkommen, dass das Opfer versehentlich schon verschlüsselte Dateien ins Backup verschiebt. Da helfen nur Backups, die schon vor der Infektion passiert sind und seitdem nicht mehr angefasst wurden, oder Formate, welche der Schädling nicht als Backup erkennt – etwa verschlüsselte Dateien oder Windows-Wiederherstellungspunkte. (fab@ct.de)

c't Download der Datenretter: ct.de/ywrb

Opfer von Krypto-Trojanern können ihre Daten mit dem Ransomware Response Kit eventuell noch retten.