Google-Geheimnisse auf Second-Hand-Router

Käufer eines generalüberholten Juniper-Routers bekamen mehr, als sie erwartet hatten: Im Speicher des Geräts stießen sie auf Konfigurationsdateien des Vorbesitzers – Google. Die Dateien enthielten sensible Informationen über das interne Google-Netz, darunter VPN-Zugangsdaten. Damit hätte man sich vermutlich Zugriff auf das Google-Intranet verschaffen können.

Martin Kluge und Florian Heinz erwarben den Juniper-Router des Typs J6350 im Frühjahr bei einem deutschen Online-Shop, der sich auf den Handel mit generalüberholter Netzwerk-Hardware spezialisiert hat. Bei der Inbetriebnahme zeigte sich, dass das Gerät offenbar nicht vollständig auf Werkseinstellungen zurückgesetzt wurde.

Eine anschließende Analyse förderte schließlich die Konfigurationsdateien mit vertraulichen Daten des Vorbesitzers zu Tage. Nachdem sich die beiden mit Google in Verbindung gesetzt hatten, zahlte das Unternehmen einen Finderlohn in Höhe von 5000 US-Dollar. (rei@ct.de)

c't Ausführliche Analyse: ct.de/y1ud

Auf einem in Deutschland gekauften Gebraucht-Router befanden sich sensible Zugangsdaten des Internet-Riesen Google.

Weitere Stagefright-Lücken gefährden Android

Die Entdecker der Stagefright-Lücken meldeten sich zurück und legten zwei weitere kritische Schwachstellen offen, über die Android-Geräte angreifbar sind. Davon sollen alle Android-Versionen betroffen sein.

Über die Schwachstellen können Angreifer abermals mittels präparierter MP3- und MP4-Dateien Geräte kompromittieren, eigenen Code ausführen und etwa Smartphones in Wanzen verwandeln. Die Infektionswege sind dabei vielfältig, warnen die Entdecker der Lücken: Angreifer können Geräte über eine präparierte Webseite oder App entern.

Mindestens eine der Lücken soll Android seit der ersten Version mitschleppen. Die Entdecker konnten Geräte mit der Android-Version 5.0 und höher erfolgreich attackieren. Google hat die Lücken bereits im Android-Code gestopft und bietet abgesicherte Firmware-Images für seine Nexus-Geräte an. Geschützt sind alle Builds ab LMY48T. Auch die Entwickler der alternativen Android-Distribution CyanogenMod (CM) haben reagiert und die Google-Patches in die CM-Nightlies eingepflegt. Wer weder ein Nexus-Gerät noch CyanogenMod nutzt, ist auf die Gunst des Geräteherstellers angewiesen – und muss sich wahrscheinlich in Geduld üben: In der Firmware vieler Androiden wurde noch nicht mal der erste Schwung Stagefright-Lücken geschlossen, der seit Ende Juli bekannt ist.

(des@ct.de/rei@ct.de)

Router-Virus dichtet Schlupfloch ab

Der Schädling Linux.Wifatch legt ein ungewöhnliches Verhalten an den Tag: Nachdem er Router und andere Embedded-Geräte erfolgreich infiziert hat, macht er sein Schlupfloch zu, um weitere Infektionen zu verhindern. Bösartige Aktionen führt Wifatch laut einer Analyse der Antivirenfirma Symantec nicht aus.

Wifatch verbreitet sich offenbar hauptsächlich über das Telnet-Protokoll. Bei der Infektion werden diverse Standardpasswörter wie „password“ durchprobiert. Kommt es dabei zu einem Treffer, nistet sich der Schädling ins Linux-System ein. Anschließend dichtet er den Telnet-Zugang ab. Die infizierten Geräte sind über ein Peer-to-Peer-Netz verbunden, über das sie Befehle vom Wifatch-Entwickler entgegennehmen können.

Gegenüber Symantec erklärte der mutmaßliche Wifatch-Entwickler, dass er keine bösen Absichten hege. Es sei ihm lediglich darum gegangen, zu lernen und für Sicherheit zu sorgen. Trauen solle man ihm jedoch nicht – stattdessen sollten Betroffene ihre Router absichern. Symantec schätzt, dass Zehntausende Geräte mit Wifatch infiziert sind, die meisten davon in China, Brasilien, Mexiko und Indien. (rei@ct.de)

Sicherheits-Notizen

In **VMware vCenter Server und ESXi** klaffen kritische Sicherheitslöcher. Abhilfe schafft ein Update auf die jeweils aktuelle Version.

Version 3.0.18.1 der Voice-Chat-Software **Teamspeak** schließt eine Sicherheitslücke, durch die Angreifer beliebige Dateien auf die Client-PCs hochladen und unter bestimmten Umständen auch ausführen konnten.

Die Entwickler des TrueCrypt-Forks **VeraCrypt** haben in Version 1.15 zwei Schwachstellen geschlossen, über die Angreifer sich höhere Benutzerrechte verschaffen können.