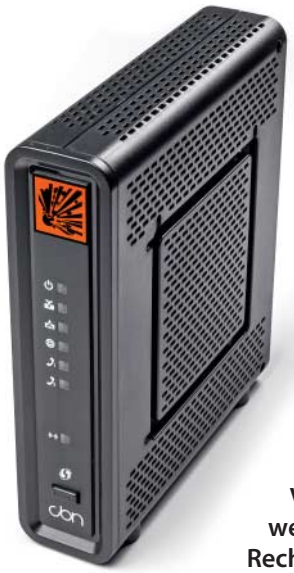


Ronald Eikenberg, David Wischnjak

Verwundbare Zwangsrouter

Gefährliche Lücken in Kabel-Routern von Vodafone/Kabel Deutschland

Gleich durch zwei Sicherheitslücken können Angreifer in die Netze der Kabel-Kunden von Vodafone einsteigen. Der Provider spricht von weit unter 1000 betroffenen Kunden, laut c't-Recherchen sind es vermutlich weit über eine Million.

Wer über das Kabelnetz von Vodafone (ehemals Kabel Deutschland) online ist, nutzt dafür einen vom Provider vorgeschriebenen Miet-Router. Die Basismodelle stellt das Unternehmen seinen Kunden über die Vertragsdauer kostenfrei – allerdings nur mit softwareseitig gesperrtem WLAN-Modul. Will man kabellos über den Kabelanschluss surfen, kann man die WLAN-Schnittstelle für zwei Euro monatlich freischalten lassen oder alternativ einen eigenen WLAN-Router hinter die Provider-Hardware hängen. Für die erste Option haben sich laut Unternehmensangaben mehr als die Hälfte der rund 2,7 Millionen Kunden entschieden.

Wie eine Untersuchung von c't ergab, holen sich diese Kunden mit der WLAN-Option nicht nur kabelloses Surfvergnügen, sondern auch ein handfestes Sicherheitsproblem ins Haus: Durch zwei Schwachstellen in verbreiteten Standard-Routern des Providers lassen sich die Netzwerke der Kunden kapern. Ein Angreifer in Funkreichweite kann so nicht nur mitsurfen, sondern auch den Datenverkehr mitlesen und manipulieren. Ferner kann er die im Heimnetz angemeldeten Geräte attackieren.

Bei den betroffenen Routern handelt sich um das Modell CVE-30360 von Hitron und den CH6640E von Compal Broadband Networks (CBN). Vodafone gibt darüber hinaus auch noch einen Technicolor-Router an seine Kunden aus, der unseren Beobachtungen zufolge jedoch nur eine geringe Verbreitung hat. Ob auch dieses Modell anfällig ist, konnten wir aus diesem Grund nicht überprüfen. Wer monatlich fünf Euro investiert, bekommt eine Kabel-Fritzbox, die nicht betroffen ist.

Taschenrechner knackt WLAN

Die beiden Sicherheitslücken klaffen in der WPS-Implementierung der Router. WPS (Wi-Fi Protected Setup) erleichtert dem Nutzer das Hinzufügen neuer Geräte ins WLAN, indem er statt des oftmals langen und komplizierten WLAN-Passworts lediglich eine PIN eingeben muss. Gerade auf Smartphone-Tastaturen ist das eine echte Erleichterung. Eine weitere Spielart von WPS ist die sogenannte Push-Button-Methode, bei der auch die PIN-Eingabe wegfällt. Die PIN-Methode hat in der Vergangenheit mehrfach für Negativschlagzeilen gesorgt: So konnten Angreifer bei einigen Router-Modellen etwa ungebremst alle möglichen PIN-Kombinationen durchprobieren oder die vom Hersteller voreingestellte WPS-PIN aus der in Funkreichweite sichtbaren MAC-Adresse des Routers berechnen.

Wie c't herausfand, fällt letzteres Problem auch Kabel-Kunden von Vodafone auf die Füße: Mit einem öffentlich dokumentierten Algorithmus konnten wir von der MAC-Adresse der Hitron-Router zuverlässig auf die voreingestellte WPS-PIN schließen und damit das WLAN-Passwort im Klartext abrufen. Ein Angreifer kann sich auf diese Weise im Handumdrehen Zugriff auf das Netzwerk betroffener Kunden verschaffen.

Dahinter steckt keine Magie, sondern lediglich etwas Mathematik: Die zweite Hälfte der MAC-Adresse (als ganze Zahl) umgerechnet von Hex- in Dezimalschreibweise und auf die letzten sieben Stellen gekürzt, ergibt die ersten sieben Stellen der WPS-PIN. Die achte Stelle ist die WPS-Checksumme und wird aus dem vorher errechneten Teil generiert. Der Angriff erfordert keine spezielle Hard- oder Software; die PIN kann man sogar mit einem Taschenrechner ermitteln.

Pixiedust-Angriff

Durch die zweite Schwachstelle konnten wir nicht nur auf Hitron-Router zugreifen, sondern auch auf das Modell von CBN. Es handelt sich dabei um die sogenannte Pixiedust-Attacke (zu Deutsch Feenstaub), die bereits vor rund einem Jahr öffentlich dokumentiert wurde. Sie ist komplexer als das oben beschriebene Sicherheitsproblem. Das macht für einen Angreifer aber kaum einen

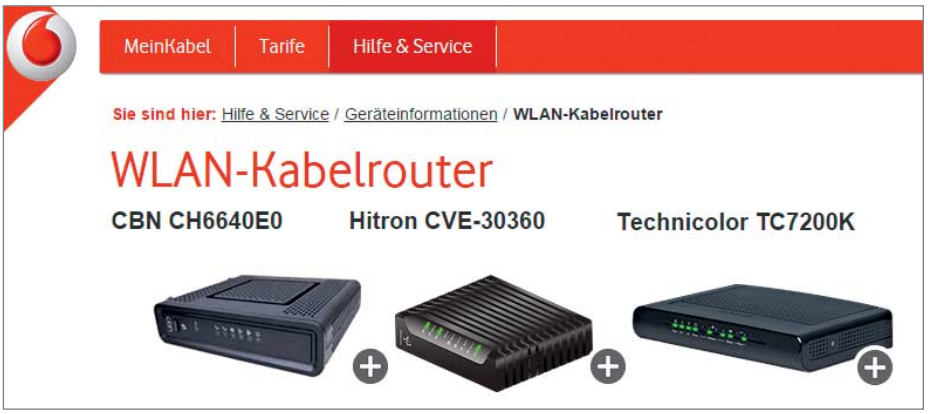
Unterschied: Die Arbeit erledigen frei verfügbare Tools wie pixiewps, das sogar zum Lieferumfang der bei Hackern und Pentestern gleichermaßen beliebten Linux-Distribution Kali gehört. Pixiedust macht sich zunutze, dass viele Router-Hersteller bei der Implementierung der WPS-PIN-Methode gepatzt haben.

Bei dieser Methode steht und fällt die Sicherheit mit der Qualität der eingesetzten Zufallszahlen. Das ist jedoch offenbar nicht bis zu allen Herstellern durchgedrungen: In vielen Fällen kommen statt echtem Zufall vorhersehbare Zahlen zum Einsatz – oder sogar einfach nur der Wert 0, wie im Fall der Hitron-Router. Ein Angreifer kann dadurch die Verschlüsselung aufbrechen und die WPS-PIN abgreifen. Mit dieser kommt er wiederum an das für den Verbindungsaufbau nötige WLAN-Passwort im Klartext – egal, wie lang und kompliziert es ist. Der Pixiedust-Angriff ist zwar aufwendiger als das Berechnen der PIN anhand der MAC-Adresse, das Knacken der PIN dauert jedoch selbst mit einem Smartphone-Prozessor nur Sekundenbruchteile. Die interessanten Details der Pixiedust-Attacke erfahren Sie im ausführlichen Hintergrundartikel auf Seite 146.

Um ein potenzielles Opfer zu finden, muss ein Angreifer nicht lange suchen: Die Router spannen bei gebuchter WLAN-Option einen Homespot genannten Hotspot auf, den auch andere Vodafone-Kunden nutzen dürfen. Über den Hotspot-Finder auf der Website des Providers und die gleichnamige App kann man deutschlandweit die Homespots auf einer Google-Karte lokalisieren – und somit auch alle potenziell verwundbaren Router.

Techniker ist informiert

Am 1. September haben wir Vodafone (damals noch Kabel Deutschland) über die kritischen Sicherheitsprobleme informiert. Das



Vodafone stellt seinen Kabel-Kunden einen von drei Standard-Routern – zwei davon waren bei unseren Versuchen akut gefährdet.

Unternehmen bestätigte unsere Beobachtungen und erklärte, dass man sich nicht darüber bewusst war, dass die Geräte von den Lücken betroffen sind. Es habe sich daraufhin mit den Router-Herstellern in Verbindung gesetzt, die „zeitnah und in guter Qualität" Software-Updates geliefert haben sollen, welche die Sicherheitslöcher stopfen. Mitte Oktober hat der Provider schließlich damit begonnen, die Updates zu verteilen. Sie sollen dafür sorgen, dass die WPS-PIN-Methode zur WLAN-Konfiguration nicht länger zur Verfügung steht. Zunächst sollen die Hitron-Router und anschließend die Geräte von CBN aktualisiert werden. Dieser Vorgang könne sich jedoch noch bis Jahresende hinziehen.

Stutzig machte uns allerdings die Angabe des Unternehmens, dass lediglich „weit unter 1000" Router von „der theoretischen Schwachstelle" betroffen seien – nämlich jene, bei denen die Kunden aktiv die WPS-PIN-Funktion zur Konfiguration genutzt haben. Eine Analyse von c't zeigt ein ganz anderes Bild: Wir stießen in der Praxis auf kaum einen Router der beiden Typen, der nicht anfällig war. Demnach muss man davon ausgehen, dass fast alle der über eine Million Kunden mit WLAN-Option über eine oder beide Schwachstellen angreifbar sind.

Vodafone will nach eigenen Angaben insgesamt 1,3 Millionen Geräte mit der abgesicherten Firmware versorgen. Kunden mit CBN-Routern können selbst aktiv werden, indem sie das anfällige WPS-Verfahren im Web-Interface deaktivieren („Gateway" / „WLAN" / „WPS"). Beim CVE-30360 hilft laut Vodafone das Aktivieren der Push-Button-Methode (PBC). Dass der Router bereits auf dem neuen Firmware-Stand ist, soll man daran erkennen können, dass im Web-Interface nicht länger die WPS-PIN-Funktion angeboten wird. Wer auf Nummer sicher gehen will, verzichtet auf die WLAN-Option und betreibt hinter der Provider-Hardware einen eigenen Access-Point – das spart langfristig auch noch Geld. (rei@ct.de)