Contents

Overview

The KRACK vulnerability was announced on 10/17/2017 and it is the most significant networking vulnerability since Heartbleed. It is documented here [1] by it's finder. The vulnerability allows an attacker that is within wifi range of the Access Point and the wifi client to tap into a connection made with WPA2 and see the unencrypted data going over it. This attack is primarily a client attack. dd-wrt contains client wireless code that is used for certain operations (repeating, etc) and is thus vulnerable. dd-wrt does NOT support 802.11r-2008 Fast Roaming which means it's server code is not vulnerable. (many commercial AP's do, however)

NOTE: THIS ATTACK DOES NOT ALLOW THE ATTACKER TO OBTAIN THE PRE-SHARED KEY ("wifi password")

While it is true that these same issues exist on WiFi networks that do not have encryption turned on, the user does get a warning message from their operating system when connecting to one of those networks.

DD-WRT firmware KRACK fix

- For any Brainslayer or Kong build:
  - Broadcom: 11-16-2017-r33772 or later
  - All others: 10-25-2017-r33607 or later

Location of vulnerability in DD-WRT

DD-WRT vulnerability depends on the router model version's chipset.

- Non-Broadcom routers use hostapd, with fixes applied for wpa_supplicant and [hostapd https://w1.fi/]. Initial fixes were in build 33525, but completely in 33555. See here
- Broadcom routers were affected in the proprietary nas module, so driver releases from Broadcom were required. Initial fixes were in build 33607, but had widely reported wireless problems. The Broadcom fixes were completed in ?SVN 33678, including for k26 (33655) & k24 (33656). However, build 33679 is missing many files, so it is recommended to use 33772 or newer.
- For chipset details, see Supported_Devices and search at wikidevi.com
- To check directly from the DD-WRT GUI, click *Administration->Commands* and put in the command "ps" then click Run Commands, if the output has "nas" or "nasmodern" it is a Broadcom

router.

Note: there is no fix for VINT builds (e.g. Linksys WRT54G v1 and v2 devices) but BS builds support VINT devices anyway

Build recommendations

Note that Repeater Bridge has been broken in the K2.6 builds after build 26125 for Broadcom devices (it works in K3.x builds) due to wireless driver issues. Client Bridge works. So if you need that you must move to K3.x builds to have the vulnerability fixed or downgrade to K2.4 builds (if your device supports it)

Some have reported that post-33525 builds are significantly faster. Build 33555 and 33607 are also slightly smaller than 33525 and their builds fit on certain routers that have slightly smaller main partitions (e.g. Netgear).

IPv6 was broken in build 33555 and only K2.4 and Mini (both lack IPv6) should be used in that build. Build 33607 had some issues with wireless radios particularly on dual radio devices and should be avoided. IPv6 was fixed in build 33679 however that build is larger than 33555 and Mega and std_nokaid_small versions of that build MAY NOT LOAD on a number of devices (primarily certain Netgear devices which reserve some of the flash in a separate partition) both 4MB and 8MB flash devices are affected.

It is not necessary to upgrade production routers UNLESS they are vulnerable (ie: used as a client bridge or repeater) ALWAYS search the BUILD thread in the forum for your router to see if someone has tested on it.

Extent of vulnerability

Some of the locations that are affected:

- Closely spaced residential homes: in many cities the average home can see dozens of SSID advertisements from neighbor's wireless routers.
- Apartment buildings, multiplexes, duplexes and other shared housing situations
- Multi-tenant commercial buildings, coffee shops, airport waiting rooms, hotels
- Hospitals and medical wifi networks

Examples of types of WiFi access points and routers potentially affected:

- Any dd-wrt router running Brainslayer builds older than build 33525 (10/17/2017) or any obsolete builds (old Kong builds, Eko builds, and one-off builds such as the CrushedHat IPv6-in-4MB build as well as personal builds created by users from source before 10/17/2017. Some devices require older and specialty builds due to bugs in newer builds (ie: wl1 failing to work in the Linksys WRT 610N v1 in newer builds)
- Any AP or router running any firmware released before 10/17/2017 that supports client bridging, or 802.11r AKA fast roaming, this includes ISP-supplied cable modems, DSL modems, etc.
- Devices running OpenWRT released before the vulnerability announced
- OpenWRT devices modified to support 802.11r this way[2]
- Any other wireless AP that defaults to 802.11r turned on, such as cellular "hotspot" devices, cellular phones configured for tethering, vehicle cellular devices that provide WiFi for vehicle occupants, etc. (some of these devices have no reason to turn FT on but might have it on inadvertently)

The finder of the vulnerability initially announced he is working on tools that will allow AP's and clients to be checked for the presence of the vulnerability. There are now a set of scripts here [3] that can be run on Kali Linux [4] that check for the vulnerability.

Types of WiFi clients affected:

- All cellular phones running Android or iOS or Windows Phone that have not been patched. Apple issued patches for KRACK on 10/31/17 in iOS 11.1 and macOS 11.13.1. Google released KRACK patches in it's 11/6/17 security update [5] but as most phones Android OS is supplied by phone vendors, individual phones may take months to be patched (or may never be patched if the manufacturer doesn't want to support them). Microsoft released a patch for Windows.
- Industrial scanning guns that use WiFi (handheld barcode scanners, etc.)
- Mobile medical scanners and other medical systems that use WiFi networks
- Unpatched operating systems that the users have disabled automatic patching
- Obsolete operating systems (Windows XP, older MacOS X)

In theory it should be possible to design a virus that would hijack a user system and allow it to attack other systems on it's wifi network using this vulnerability.

Impact to DD-WRT

There are dozens if not hundreds of models of WiFi routers that will NEVER be patched by their manufacturers, either due to the manufacturer no longer existing, or the manufacturer refusing to release updates. For example the purchase of Linksys by Cisco then the selling of Linksys to Belkin created tens of orphaned models. There are MANY wifi vendors who refuse to devote programmer time to rebuild firmware for models that they have stopped selling. Some, such as Cisco, have formal End Of Life processes where the company unequivocally states that after EoL date, NO further firmware updates will be provided.

While it is probably a truism that the majority of residential users probably think a firmware file is a manila folder, there is a serious issue with businesses. Many businesses have a "patch or toss" approach and if a device is considered obsolete by it's manufacturer with no firmware forthcoming, the business has no choice but to retire the gear.

It may be that this will see increased use of dd-wrt in businesses. It may also be that there will be a flood of used WiFi gear that comes on to the market as a result of accelerated gear retirement. Certainly there will be increased interest in dd-wrt as a way of prolonging gear service life.

Mitigation steps other than patching clients and routers

Encrypting the data from the application to the server by the PC or phone operating system before transfer over the wifi network is one other way to protect against a KRACK attack. https, SSL IMAP and POP3, and VPN clients running in the client operating system are some examples of how this can be done.

Atheros-based dd-wrt routers can disable EAPOL Key Retries to block these attack as discussed here: Disable EAPOL Key Retries

Disable any client access in dd-wrt. Because dd-wrt does not have 802.11r support (fast roaming) it's AP server code is not vulnerable so if it is configured only as an AP (repeater functionality turned off) the

vulnerability is not exploitable against the AP. (it IS still exploitable against the client if the client isn't patched)

Kong announced on 10/18 "There will be an option in the webif in the next build, that allows to set an flag that will fix that issue even if the client does not have a patch, but it can cause interoperability issues and therefore is off by default." in this [6] thread. The option was set a day later here [7] into the build system.

Note: setting MAC Address filtering DOES NOT protect against this attack!