

update for sp2?

--whiteboy 06:07, 3 Oct 2006 (CEST)

Hello MrElvey,

Thanks for contributing to the article :)

The main issue with *user-generated* hashes, is that there is no way to verify that the hash is correct (even when using an encrypted https/ssl connection). It is entirely possible that a *user-generated* hash was generated from a corrupt firmware file downloaded from dd-wrt's website. This is precisely why the hashes **must** be posted by the developers themselves (and as I have mentioned, Eko has begun doing just that). All a *user-generated* hash really tells you is that the firmware file you downloaded matches the firmware file another user downloaded... and if that other person has tested the firmware reliably, you can, with *marginal* assurance, assume it is not going to brick your router.

The encrypted connection would put an extra layer of security around the hashes, however it still does not solve our original problem of the user-generated hashes themselves.

Perhaps you realize this already, but just thought I would mention it for our users.

--Soulstace 09:02, 17 January 2008 (CET)

Yup, I am aware of that issue, but it's not the only issue; MITM is of concern too. Came here to get the latest (24sp1) and can't find valid hashes for it.

downloaded

https://secure.dd-wrt.com/dd-wrtv2/downloads/stable/dd-wrt.v24%20SP1/Broadcom/Linksys/WRT54GL_1.1/ as well as..

https://secure.dd-wrt.com/dd-wrtv2/downloads/v24-sp1/Broadcom/Broadcom%20Generic/dd-wrt.v24_voip_g but found that both were identical, but couldn't find a matching hash:

```
% md5 dd-wrt.v24_voip_generic.bin
MD5 (dd-wrt.v24_voip_generic.bin) = 46715d41e52b1577eb7d97f433cc8249
% openssl sha1 dd-wrt.v24_voip_generic.bin
SHA1(dd-wrt.v24_voip_generic.bin)= 3030459ff1285f57bce4b91539bfb0ea194e1333
```

However, <https://secure.dd-wrt.com/dd-wrtv2/downloads/v24-sp1/MD5SUMS> doesn't have those hashes; it has DIFFERENT ones!?!

Not to mention that the download site has gotten worse - now it's more difficult to get anything over https; now the https site keeps serving up pages directing the user to the http version.

What's up with that?? :(

-MrElvey 05:08, 1 August 2008 (CEST)

As of this moment the v24 SP1 hashes have not been published. I contacted the developers about it.

FWIW, the MD5SUM of my voip_generic is also 46715d41e52b1577eb7d97f433cc8249. So you're probably O.K. to flash.

P.S. - You can grab the files from the Generic Broadcom section. No need drilling down any further.

--Soulstace 03:53, 3 August 2008 (CEST)