# Installation Media - Bug #1501

## should the ISOs download links redirect to mirrors?

2017-10-15 12:01 PM - marco

| | | | |
|---|---|---|---|
| **Status:** | fixed | **% Done:** | 0% |
| **Priority:** | discussion | | |
| **Assignee:** | bill-auger | | |
| **Category:** | | | |

**Description**

On https://wiki.parabola.nu/Get_Parabola#Preview.2FBeta_Releases the SHA512SUM links do not work.  First one links to https://repomirror.parabola.nu/iso-beta/systemd-lxde-2017.10.04/SHA512SUM and is a 404.

Additionally, would it not be better to not link to a mirror but have the checksums hosted on a central, trustworthy, maybe independent host?

### History

**#1 - 2017-10-15 06:41 PM - bill-auger**

i have corrected the dead links - thanks for reporting this

i asked that question myself on the wiki talk page a few days ago https://wiki.parabola.nu/Talk:Get_Parabola#why_.3Fnoredirect
i have been hoping to get a few opinions about this before making any final decision on how the downloads and torrents will be managed

```
all of the download links are of the form repo.parabola.nu/iso/edition/file?noredirect

why not? repomirror.parabola.nu/iso/edition/file

is this a security concern? - if so then the existence of the torrents would seem to betray that notion

the main releases and their checksums are GPG-signed so there is no security concern regardless of where the f
iles are hosted - all of the mirrors host the ISOs - if the parabola downloads page does not utilize them then
 they are probably just taking up space and will never be accessed at those locations - ideally all of the mir
rors would become bittorrent web-seeds and ideally all users would want to use bittorrent and therefore be dow
nloading from any or all mirrors simultaneously
```

**#2 - 2017-10-15 06:42 PM - bill-auger**

*- Description updated*

**#3 - 2017-10-15 06:45 PM - bill-auger**

*- Priority changed from broken to discussion*

*- Assignee set to bill-auger*

*- Status changed from open to info needed*

*- Subject changed from checksums are dead links to should the ISOs download links redirect to mirrors?*

**#4 - 2017-10-15 07:39 PM - isacdaavid**

bill-auger wrote:

> i asked that question myself on the wiki talk page a few days ago https://wiki.parabola.nu/Talk:Get_Parabola#why_.3Fnoredirect

makes sense to me. i don't think the addition of ?noredirect was motivated by security concerns. the former maintainer just got carried away.

having no ?noredirect also raises the question of whether an "HTTP mirrors" section is necessary at all. maybe some people will still want to go to a mirror of their choice.

marco wrote:

> Additionally, would it not be better to not link to a mirror but have the checksums hosted on a central, trustworthy, maybe independent host?

only marginally. you aren't supposed to trust any server at their word for the checksums, not even the central one. check signatures with gpg, then you can trust the contents of the signed file (whether the checksum file or the .iso itself) to the extent that you trust the signing key.

that said, i'm seeing that not all of the beta ISOs (or their checksums thereof) have been signed. also, the CLI versions have both .iso and checksums signed (which is redundant but not problematic), whereas the OpenRC versions sign .iso but not checksums (rendering checksums redundant).

#### #5 - 2017-10-15 08:29 PM - bill-auger

isacdaavid wrote:

> i'm seeing that not all of the beta ISOs have been signed.

ive added links to signatures to all of the preview ISOs

that was not so much an oversight but for convenience - with so many files associated with each ISO the managing all the download links is quite unwieldy - i do agree that the checksums do not need to be signed (the checksums themselves are redundant - yes?) so maybe if we sign only the ISO that would reduce the number of files associated with each ISO from 6 to 4

i wrote a PHP script to fetch the latest versions of these based on the dates in the filenames so that the download links would not need maintaining but i have not installed it - that would help maintaining the download page a lot - my main concern has been the ISOs themselves - the download page is more of a lower priority design/usability concern which i have not given much thought to yet - anyways that is why we have not been adding all of the auxiliary files

#### #6 - 2017-10-15 09:34 PM - marco

I agree that checking the gpg signature is the way to check the trustworthyness of the ISO file.

It could still be useful for some users to have a simple checksum to check the file's integrity.  This would be done implicitely by checking the gpg signature on the ISO, but is (a bit) more of a hassle.

#### #7 - 2017-10-15 09:44 PM - bill-auger

marco wrote:

> It could still be useful for some users to have a simple checksum to check the file's integrity.

yes in fact there are 2 checksums posted with each of the main releases - that protocol will continue - the question was whether the checksums themselves also need to be signed

some of these were neglected for the preview releases because they will all be short lived and replaced often - once they graduate to the main releases section each will sirely be signed and be accompanied by 2 checksums

#### #8 - 2017-10-16 05:56 AM - isacdaavid

bill-auger wrote:

> the question was whether the checksums themselves also need to be signed

signing checksums alone is sufficient to cerfify that the ISO hasn't been tampered with: you verify the checksum file with gpg, then hash the ISO to see that it matches what the checksum file claims. i believe the oldest of all existing installation media (Mate/Systemd) does this, that was the previous ISO maintainer's workflow.

marco is asking for continuing that method, i think.

the alternative renders obsolete not only checksum file signatures as you point out, but also checksum files themselves. you sign the whole ISO alone, and verifying its signature amounts to knowing that it hasn't been tampered with

#### #9 - 2017-10-16 06:42 AM - bill-auger

the existing main releases published the ISO and 2 checksums plus signatures for all 3 of those for a total of 6 files per release - i discussed this with megver and we agree upon the reasoning for 2 checksums - they exist for the sake of those without gpg or the ultra-paranoid - this is just to make clear that both checksums are strictly redundant so surely those do not need signatures - so to agree that 4 files per release is more than sufficient even by the most extreme standards (the ISO, the ISO.sig, a sha256sum, and a whirlpoolsum)

#### #10 - 2017-10-16 09:04 AM - marco

Yes, it seems redundant already (and that's fine).  I would suggest not to change anything of the working procedures.

I'm sorry for deviating from the original issue (which is solved); this can be closed as far as I'm concerned.  Related to this, I have put a small issue on the talk page: [https://wiki.parabola.nu/Talk:Get_Parabola#Check_sums_and_GnuPG](https://wiki.parabola.nu/Talk:Get_Parabola#Check_sums_and_GnuPG)

**#11 - 2017-10-19 11:14 PM - bill-auger**

*- Status changed from info needed to fixed*