Packages - Privacy Issue #3265

[your-privacy] List of packages which implement UPnP should be added to the blacklist

2022-04-28 01:57 PM - gap

Status:	confirmed	**% Done:**	0%
Priority:	privacy issue		
Assignee:			
Category:			

Description

UPnP is not a particularly secure protocol, unless you configure extra layers of security on top of it.

The following packages which implement UPnP should be added to the blacklist:
- gerbera
- gupnp
- gupnp-av
- gupnp-dlna
- gupnp-igd
- gupnp-tools
- libupnp
- libupnp-debug
- mediatomb
- minidlna
- miniupnpc
- miniupnpd
- python-miniupnpc
- rygel
- ums

This list may not be exhaustive.

History

#1 - 2022-04-30 09:06 PM - bill-auger

- Priority changed from bug to privacy issue

- Status changed from unconfirmed to confirmed

- Description updated

#2 - 2022-04-30 10:39 PM - bill-auger

the one concern that jumps out at me immediately, is to avoid confusing privacy with security - UPnP is much more of a security concern than a privacy concern - privacy problems would be due to clients which are designed that way as a feature - if any parabola package was known to have such privacy-invading mechanism, that one would be an obvious candidate for 'your-privacy'; but these clients are all libre, so they most likely would not have such features - flash player for example, was most notorious in that way

maybe there could also be a 'your-security' blacklist; but the main security problem is the fact that UPnP is enabled on the network router - in other words, anyone who is concerned about the security implications of UPnP, should simply disable it on the router

im not exactly a networking expert - id like to get more opinions about this

#3 - 2022-04-30 11:50 PM - gap

To add insult to injury, Flash Player is proprietary as well as horrifically insecure.
Whilst we're on the topic of Flash, there is a project to write a libre implementation (https://ruffle.rs).
(AFAICT GNU Gnash hasn't been updated in years.)
Unfortunately, most of the things that use Flash are proprietary anyway, which is a shame, so it doesn't look like being able to use Flash media will be much of a benefit to the free world, especially since it's a now-deprecated medium.
The recent attempts to archive Flash media have also been plagued by certain proprietors requesting the archival projects take down the works they authored, especially in the case of one company I will not name because I do not wish to promote it.

As for disabling UPnP on the router, not everybody has control over the router they are connected to, especially if it is a public router, so it would be best to also disable it on the local computer.

I agree with the point about conflation.
If this is the preferred solution then your-privacy should depend on your-security, since privacy depends on security, which is why I proposed adding it

to the existing your-privacy package.
I didn't know how well the idea for a new package would go down, especially since we have a lot to maintain already.

If we are going to make this new your-security package, then I'd suggest we start to migrate from OpenSSL over to LibreSSL, although a project that large should go upstream.
I think Hyperbola started building their repos against LibreSSL also, although I'm not sure.

This issue reminds me of #2619 (improving and renaming the nonprism repo) as well.

#4 - 2022-05-01 12:34 AM - bill-auger

> I agree with the point about conflation.
> If this is the preferred solution then your-privacy should depend on your-security, since privacy depends on security

that is just not true - it is the same conflation - privacy depends almost entirely on the user's own diligence and self-restraint - 99% of privacy problems relate to use of a web browser - but the web browser is not the source of the privacy problems - the source is the particular websites that people visit

someone could maintain perfect privacy on a system that is completely insecure - it does not matter which software is used, it matters what the user chooses to do with the software (primarily, which other computers the software connects to) - if some software connects to other computers without the user's knowledge, that would be an anti-feature; and that software would be need to be treated, per the FSDG - but if some software connects to someone else's computer, because the user's chose to do so, the user has voluntarily forfeited privacy, in every case - there are privacy tools such as tor which can help - security tools can do very little, unless the user learns how to use them properly

security is a matter of preventing other computers from making changes to the local computer or stealing secrets from the local computer - privacy is a matter of other people learning what you do with your computer - security is not going to help with that very much - privacy is much more easily invaded on the other computer, out there "in the cloud"; because in most cases, that is "what people do with their computers" - they connect to other people's computers - that is entirely what most people in the libre community mean by "privacy" - the way to protect it, is to avoid connecting to that other computer, and to keep any personal information secretly (encrypted, on an external storage, etc), just in case there is a security hole on the local computer - that is very unlikely, and for someone "out there in the cloud" to be interested on someone's local files, is even less likely

from my experience, most people who care about internet privacy, do not care about security at all, and they have no reason to - they simply misunderstand what computer security is - both are a matter of "defining your threat model"; and most people's threat model is grossly uninformed - education is the solution, not protection

> I didn't know how well the idea for a new package would go down, especially since we have a lot to maintain already.

these are not software packages, only a list of conflicts against other packages - the maintenance burden is negligible

> This issue reminds me of #2619 (improving and renaming the nonprism repo) as well.

it reminds me of nonprism also - much of what i worte above is re-iterating the rationale for the #2619 proposal - the solution is the same: parabola should stop giving the illusion of protection - these blacklists should be considerd as guidance, which the user must learn more about, in order to be effective

parabola is about the furthest thing from tails or qubes on the spectrum of OSes - parabola gives users the tools to implement those privacy and security measures on parabola; but nothing like that is implemented by default - the default is to be libre, not private nor secure - those things require diligence and knowledge on the user's part - if the defaults were so strict, it would not be very "arch-like" - people who are worried about privacy or security, but are not very knowledgeable of such things, should not be using any rolling distro - an LTS distro is much more appropriate for such people

#5 - 2022-05-03 03:00 PM - gap

A conflation would be claiming security and privacy are the same thing, wheras I'm just claiming that privacy depends on security.
We can't expect everybody to be knowledgeable or incessantly vigilant about freedom, security, and privacy, which is why the respective your-* packages exist.
Unless we expect the user never to connect to another machine (which is the vast minority in today's world of the internet), a private machine necessarily has to be secure, because an insecure system could be cracked or leak data, which is a violation of privacy if the data in question is private, which it almost certainly is.

In any case, I agree all Parabola can do in order to protect its users is imperfect, and we should do more to educate them, perhaps on wiki articles.