Packages - Freedom Issue #411

[iceweasel] [icecat] enable tls 1.1 on pkgver >= 23

2013-09-20 08:55 AM - fauno

Status:	not-a-bug	**% Done:**	0%
Priority:	feature		
Assignee:			
Category:			

Description

From http://www.hiawatha-webserver.org/weblog/58

> Firefox 23 supports TLS/1.1... finally!!
> 7 August 2013, 14:40
>
> Mozilla finally decided to include TLS/1.1 support in Firefox. However, most users won't benefit from this support, because it's disabled by default and enabling is not many people will and can do. To enable TLS/1.1 support, use "about:config" in the URL bar and search for the security.tls.version.max setting. Set its value to 2 (default is 1).
>
> Happy secure browsing!

History

#3 - 2013-09-21 12:29 AM - lukeshu

I'm all for encouraging privacy, and being on the bleeding edge, but I think this is a bad idea. From this standpoint, the Mozilla people know what they're doing. If they chose to not enable it by default, they had a good reason for it. We want to trust some blog post instead of the collective knowledge of all the cryptogophers at Mozilla?

#4 - 2013-09-21 01:34 AM - Anonymous

iceweasel-libre 24 version should be possible to enable TLS 1.1, but there are 2 open issues that prevent us from changing the default to enable it:
- Compatibility with servers that are not tolerant to sending TLS 1.1 => https://bugzilla.mozilla.org/show_bug.cgi?id=839310
- Prevent downgrade attacks => https://bugzilla.mozilla.org/show_bug.cgi?id=861310

#5 - 2013-09-22 08:08 AM - fauno

lukeshu wrote:

> I'm all for encouraging privacy, and being on the bleeding edge, but I think this is a bad idea. From this standpoint, the Mozilla people know what they're doing. If they chose to not enable it by default, they had a good reason for it. We want to trust some blog post instead of the collective knowledge of all the cryptogophers at Mozilla?

according to the bug emulatorman linked, they're not worried about security but compatibility, since 1-2% of global webservers don't support tls 1.1 yet.

#6 - 2014-02-11 02:55 PM - fauno

http://www.cryptofails.com/post/70233715224

```
So, in summary, it took Mozilla four years to realize they had to
 implement TLS v1.1 after it was standardized. Once they did, it took two
 years to implement, and then another year just to get it turned on by
 default. I honestly don’t know why it took so long.
```

```
The [other major browsers][] (Chrome, IE, Opera, Safari) all had support
 for both new versions, turned on by default, by at least October 2013.
 Notably, Google Chrome had TLS v1.1 up and running all the way back in
 September of 2012.
```

```
The other browsers did much better than Firefox, but none of them did
 exceptionally well. We should all be ashamed of how long it has taken
 our browsers to give us the newer versions of TLS that we desperately
 need. We can only hope that future versions of TLS will get turned on
 much quicker.
```