

## TYPO3.Flow - Task # 36050

<b>Status:</b>	Rejected	<b>Priority:</b>	Should have
<b>Author:</b>	Aske Ertmann	<b>Category:</b>	Core
<b>Created:</b>	2012-04-14	<b>Assigned To:</b>	Karsten Dambekalns
<b>Updated:</b>	2012-05-15	<b>Due date:</b>	
<b>Sprint:</b>			
<b>PHP Version:</b>			
<b>Has patch:</b>	No		
<b>Complexity:</b>			
<b>Subject:</b>	Raise the minimum PHP version due to security issues		
<b>Description</b>	<p>We should consider raising the minimum PHP version requirement in the Bootstrap since there is a security issue concerning null byte poisoning for all file functions. Since there is no sanitizing in FLOW3 concerning the null byte poisoning, we should raise the requirement to 5.3.4, since it is fixed in that release.</p> <p>Another suggestion is to raise it to 5.3.6 and get rid of the PDO charset handling.</p>		

### History

#### #1 - 2012-04-14 17:34 - Karsten Dambekalns

- Status changed from New to Accepted

#### #2 - 2012-04-14 17:35 - Karsten Dambekalns

- Tracker changed from Suggestion to Task

- Project changed from TYPO3 Flow Base Distribution to TYPO3.Flow

#### #3 - 2012-04-14 17:35 - Karsten Dambekalns

- Category set to Core

- Has patch set to No

#### #4 - 2012-04-17 16:03 - Adrian Föder

I personally agree, but I wanted to mention that many "distributions" contain a PHP 5.3.3 out of the box (i.e. Debian Lenny and some MAMP or something iirc). Also, checking the usage of 5.3 world-wide says 5.3.3 is the most minor one used.

But, as also stated at the T3DD12, I'm fine with just forcing 5.3.6 with saying "it's an enterprise framework".

I'm sure it won't run on various simple, hosted environments for many other reasons than the 5.3.6.

#### #5 - 2012-05-04 20:56 - Jacob Floyd

I'm on a shared host, and I think these cheaper hosts are a great path to get FLOW3 into enterprise environments. If hobbieists pick it up and use it on their personal projects, then they'll also recommend using it when they go to work, because they'll know how much fun it is to use.

As for 5.3.6? Works for me. My shared host is on 5.3.10 :) So, I agree with the conclusion, go ahead and jump to 5.3.6, but I just don't agree with the reasoning. FLOW3 is much more than **just** an *enterprise* framework. It is very versatile and can be used to solve many problems big and small. If we restrict ourselves to the 'Enterprise' market, then TYPO3 is never going to grow much bigger than it is. (Note I said, market not quality. I fully support making things of enterprise quality for all markets).

**#6 - 2012-05-15 00:06 - Jacob Floyd**

Just to clarify:

"raise it to 5.3.6 and get rid of the PDO charset handling"

is referring to php#47802 that landed in 5.3.6, right?

<https://bugs.php.net/bug.php?id=47802>

Also, distros like RH and CentOS backported the NULL point security issues to 5.3.3, right? So, is 5.3.4 necessary for those distros?

I ask because I want to upgrade PHP on a server at work, and I'm getting some push back, because they only want to use yum to keep things up to date.

Then again, maybe I should just make a Surf recipe to update PHP and not manage it with the system package manager...

**#7 - 2012-05-15 09:41 - Karsten Dambekalns**

Hi Jacob.

Jacob Floyd wrote:

*"raise it to 5.3.6 and get rid of the PDO charset handling"  
is referring to php#47802 that landed in 5.3.6, right?  
<https://bugs.php.net/bug.php?id=47802>*

Yes.

*Also, distros like RH and CentOS backported the NULL point security issues to 5.3.3, right? So, is 5.3.4 necessary for those distros?*

I don't know if those backported the fix. But I remember from my years with SuSE that they did...

*I ask because I want to upgrade PHP on a server at work, and I'm getting some push back, because they only want to use yum to keep things up to date.*

Why not use something like that (30 seconds with Google, ask you admins to try that ;) )

- <http://www.webtatic.com/news/2012/05/latest-updates-php-5-4-2-5-3-12-mysql-5-5-23-5-1-63/>
- <http://www.webtatic.com/packages/php53/>
- <http://www.webtatic.com/packages/php54/>

**#8 - 2012-05-15 15:49 - Karsten Dambekalns**

- Status changed from Accepted to Rejected

We discussed this and came to the conclusion that for us the requirement is feature driven. It should be clear to everyone that having a secure infrastructure below FLOW3 is nothing we can enforce.

From the feedback we got so far it became clear that raising the requirement would be a real hassle for a lot of admins while the needed security

fix(es) are often backported by distribution vendors.