

Update notifier

Since 1.9.9, site admins have an optional weekly version check in tiki-admin.php. However, this has not always been reliable over the versions, and it lacks flexibility and a way to effectively warn people to deal with a security issue (ex.: update or deactivate X).

Todo ASAP

- [Update notifier: deal better with SVN installs](#)

Revamp 13/12

This is was a plan (which didn't happen by lack of folks helping) to revamp this feature for Tiki13, and ideally for a backport to a future 12.x in May 2014. Tiki 12 will be supported until November 2018, so it's very important to have this.

How to do the update notifier with more flexibility, while keeping it secure?

Tikis out there would check a .yaml or .json file daily / weekly / monthly / never (by default, weekly), like they do now for version numbers. In that file, we'll have all the info that each Tiki needs to inform the site admin. This file will be protected by SSL, like <https://tiki.org/stable.version>

For future security releases, we just release and update a yaml/.json file and the rest will take care of itself. (site admins being alerted if their site is vulnerable)

General message for all Tikis

This message will be shown in a rotating snippet ticker in tiki-admin.php. Could be

- New release
- New security release
- A call to action to support Tiki for an award, Next TikiFest, Bootstrap is coming, etc., whatever.

If we don't send an e-mail, it's not intrusive.

- Text snippet / sanitized HTML (sanitized by the Tiki site itself)
- Is this urgent and should be sent to site admins by email? yes/no

Rotating short snippet

[PluginScroll](#) doesn't seem to work, so either fix and use that or find another

Potential scripts

- <http://www.maxvergelli.com/docs/jquery-scroller/examples.html>
- <https://github.com/aamirafриди/jQuery.Marquee>
- <https://github.com/tetsuwo/jquery-news-ticker>

License not compatible

- <http://www.jquerynewsticker.com/>
- <https://github.com/jonmifsud/Web-Ticker/>

Preference: email setting for alerts

The email must go out even if tiki-admin.php is not visited (so this should go in tiki-setup.php?)

The email would be sent as any other e-mail from each Tiki to:

- all members of the Admins Group (default)
- the e-mail of the admin user (old installs tend to have no admin e-mail here or could have renamed this user)
- comma separated list of usernames
- comma separated list of emails
- never send mails
- in the future, SMS, XMPP, etc.

Preference: to know how Tiki is installed / managed

- Add a pref to indicate which upgrade method is used (so if a different person takes over a project, they know what to do)
 - SVN
 - SimpleScripts
 - Softaculous
 - Installatron
 - Manual upgrades
 - Unknown

This should be set by the installer, but be override-able by the admin.

Related:

[Configuration Management and Systems Orchestration](#)

Inform the Monitoring system

Nagios / Icinga / Shinken / Zabbix should be informed of this message

Preference: to indicate LTS

- Should the user indicate this so we can stop showing them upgrades to non LTS versions?

Conditional checks

To improve the [signal-to-noise ratio](#), we want site admins to be alerted to only important issues. We should be able to deal with LTS, [Auto-installers](#), etc. Only tell about updates administrators may care about.

How can this conditional syntax be useful in Tiki? Maybe something like PluginCondition or an enhancement to [PluginPref](#)?

Security

Conditions	Snippet	To be sent by email	Notes
If feature_abc is on and if version is 6.x and less than 6.9	The abc feature has a known vulnerability. To be safe, you can a) delete the tiki-abc.php file b) upgrade to 6.9 c) turn off feature_abc from the admin panel d) make sure only trusted groups can use this feature (so remove tiki_p_abc from Anonymous and any untrusted group)	yes	
If feature_abc is on and if version is 9.x and less than 9.3	The abc feature has a known vulnerability. To be safe, you can either a) delete the file tiki-abc.php b) upgrade to 9.3 c) turn off featureabc from the admin panel d) make sure only trusted groups can use abc (so remove tiki_p_abc from Anonymous and any untrusted group)	Yes	
If feature_abc is on and if version is 9.x and less than 9.3 and and Anonymous group has tiki_p_abc	The abc feature has a known vulnerability which can be exploited by Anonymous users. To be safe, you can either a) delete the file tiki-abc.php b) upgrade to 9.3 c) turn off featureabc from the admin panel d) make sure only trusted groups can use abc (so remove tiki_p_abc from Anonymous and any untrusted group)	Yes	

Upgrade is available

Conditions	Snippet	To be sent by email	Notes
If version is 11.x and less than 11.2	Tiki 11.2 is available.	no	This could even replace our current version number thing. Let's assume there is no security vulnerability fixed between in 11.1 and 11.2
If version is 11.x	Tiki 11.x is supported until the release of 12.1, which is planned for November 2013 (you should planned an upgrade around this time)	no	
version number: 10.x	You are currently using Tiki10 and the end-of-life of the 10.x series (10.3, 10.4, etc) is scheduled for May 2013	no	

version number: 6.x (before end of life)	You are currently using Tiki6LTS and the end-of-life of the 6.x series (6.7, 6.8, etc) is scheduled for May 2014.	no	
version number: 6.x (after end of life)	You are currently using Tiki6LTS and this version is no longer supported (end of life) since May 2014. You should upgrade.	yes	
version number: 9.x and LTS=y	You are currently using Tiki9LTS and the end-of-life of the 9.x series (9.3, 9.4, etc) is scheduled for November 2015	no	
version number: 9.x and LTS=n	You are using 9.x and 10.x has been released. You should upgrade or switch your system to use LTS versions to avoid these warnings	no	
version number: 9.x and LTS=y	You are using 9.x LTS and 12.x LTS has been released. You can stay on 9.x but you may want to upgrade to benefit from new features.	no	Assuming 12.2 was released

Type of installer

Conditions	Snippet	To be sent by email	Notes
installer=manual install from zip	You installed this with Installatron. To upgrade, you should follow the instructions at doc.tiki.org/Update	no	
installer=Installatron	You installed this with Installatron. To upgrade, you should use the Installatron system.	no	
installer=Fantastico	You installed this with Fantastico. To upgrade, you should use the Fantastico system.	no	
installer=svn	You installed this via svn. To upgrade, you should follow the instructions at dev.tiki.org/Update	no	
installer=SimpleScripts	You installed this with SimpleScripts . To upgrade, you should use the SimpleScripts system.	no	
installer=UbuntuPPA	You installed this with UbuntuPPA . To upgrade, you should use the UbuntuPPA system.	no	

Tracking messages that should no longer be shown

- We need a way to store what should no longer be shown (ex.: a message blacklist)
 - Email should only be sent once
 - Once a warning has been given, it should be possible to silence it.
 - There should be a way to reset all messages (ex.: for a new admin)

Privacy admin panel

- Copy all the prefs that produce an outbound request so a site admin can deactivate them all. (I am behind a firewall, and trust my users so I don't need to be alerted about these things)

Things to note

- By having one yaml/json for all the conditions, we are not tracking / disclosing what features they are using. The check/actions are done by their own Tiki. We don't know their email. They just need to update the admin email of their Tiki.
- Since this is for each Tiki, a site admin will receive an email for each vulnerable Tiki (which is a good thing because it's easy to lose track).

Questions

- Depending on if site is on LTS or not, messages will be quite different. Should we manage all this in one json/yaml file or several?

Longer term ideas

Tiki Connect

Later, we could personalize this with info from Tiki Connect. Ex.: There is a TikiFest coming in your country, a webinar in your language

Opt-in feature to let tiki.org turn off vulnerable features

This is controversial and must be very well thought out, so we will revisit this after the announcement system in 12/13 works well.

We could push even further with an opt-in program which automatically turns the feature off and sends an email.

- On weekly check, Tiki shuts off features reported insecure by tiki.org
 - version X, pref to be turned off, message to give the admin via mail and in admin panel, link to reactivate feature if you want to take your own risks

Auto-updates

See [Automatic Updates](#)

Related

- [Server check](#)
- [Releasing](#)
- [Connect](#)

alias

- [Upgrade notifier](#)