Tiki under attack

Oliver Hertel - 04 Sep 2006 06:44 GMT-0000

Maybe you already found this domain partially unavailable this weekend. Some russian hackers are attacking tiki installations currently, trying to install spam and/or DoS bots. We are working at it and hope to have solved the problems soon.

Sorry for the inconveniences.

Details and quick fix here!

How you can make your system more secure against those attacks

- Remove the file jhot.php. JGraphPad will be dysfunctional afterwards until we provide a fixed version. You can grab it from current CVS (BRANCH-1-9 or HEAD) already.
- Edit file tiki-editpage.php. If the line

□□□□□□□

```
chmod("$wiki_up/$picname", 0755); // seems necessary on some system (see move_uploaded_file doc on php.net
```

exists, remove it!

- Enable .htaccess files. Tiki comes with them already, you just have to rename them from _htaccess to .htaccess. Check first, if your webserver is supporting this!
- Fix permissions of files in the docroot. Run tiki's fixperms.sh. We're working on an improvement of that script.
- Use tiki-install.php or mysql client to import the script tiki-secdb_1.9_mysql.sql into the tiki database. With Menu / Admin security / Check all files you can run a job that validates all existing php files in tiki dir against checksums. Tiki will complain if there are more or modified files. Check those files.
- add this line to php.ini and restart apache:

□□□□□□□

```
disable_functions passthru, system, shell_exec, popen, proc_open, exec, eval
```

That's what can be quickly done. If you want more:

- chroot your apache. The attacks use perl, wget, curl... if you chroot your apache into a more or less empty tree of directories, those tries will fail.
- Maybe use hardened php to make your system even more secure.

We can't guarantee that all this is enough. But it's a start.

How you can detect if your system is corrupted already

- Another application is running on port 443. If you try to restart apache, it will complain about the port being locked. Check with ps what's running with apache userid, then go kill it.
- There might be a file img/wiki/tiki-config.php available. Thats no tiki file! If you find tmp.php, temp.php, mail.php, b9.php, vb.php, tiki-lang.php, mod_wiki.php or lang/lang.php, those are hacks, too, none of them original tiki code. Delete them! There might be other files too that are not coming with tiki.

Appendix

- howto .htaccess files
- script to enable/disable .htaccess files
- hardened php
- chroot apache
- alert on Internet Storm Center
- message on heise news