apache: /server-status page publicly visible through Tor or Pagekite

The `/server-status` page is only meant to be viewable from localhost. But since Tor onion service and Pagekite connections are treated as local, the page is publicly visible through those. (I only tested Tor, but I assume Pagekite will do the same.)

The issue was reported on IRC, so it is somewhat public knowledge already.

- [ ] Disable mod_status, or require authorization for `/server-status` location.
- [x] Make an announcement on the forum, mailing list, and social media with instructions so users running Pagekite or Tor Onion Service can quickly disable mod_status with `sudo a2dismod status && sudo systemctl restart apache2`.

Edited 2 years ago by James Valleroy

⬆ Drag your designs here or click to upload.

Tasks ◎ 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items ⊘ ▯ 0

Related merge requests ⑂ 1
⊖ apache: Disable mod_status   ⊘
!1899

When this merge request is accepted, this issue will be closed automatically.

Activity

James Valleroy added Privacy   Security labels 2 years ago

James Valleroy @jvalleroy · 2 years ago   Author Owner
Draft announcement:

Security/privacy issue for users of Tor onion service or Pagekite

An issue has been found in FreedomBox that allows anonymous and unauthorized users to access private and potentially security relevant information. The information is shown on an Apache Server Status page and includes the IP address and URL request path for clients accessing pages on the server.

By default, Apache only allows access to the Server Status page from the local machine. However, due to how Tor onion service and Pagekite are used on FreedomBox, they bypass this restriction and allow anyone to access the page.

We are planning to fix this issue in the next release of FreedomBox. However, our releases have been delayed at the moment. Therefore, if you are using Tor onion service or Pagekite, we strongly recommend that you disable the Server Status page.

You can disable the page by running the following two commands on your FreedomBox, either using Cockpit or SSH:

```
$ sudo a2dismod status
$ sudo systemctl restart apache2
```

If you have any questions, feel free to ask at any of the following locations:

- Forum: https://discuss.freedombox.org/
- IRC: irc.debian.org, channel #freedombox
- Matrix: #freedombox:matrix.org
- Mailing list: https://alioth-lists.debian.net/cgi-bin/mailman/listinfo/freedombox-discuss

James Valleroy added Next Release label 2 years ago

James Valleroy made the issue visible to everyone 2 years ago

James Valleroy marked the checklist item **Make an announcement on the forum, mailing list, and social media with instructions so users running Pagekite or Tor Onion Service can quickly disable mod_status with `sudo a2dismod status && sudo systemctl restart apache2`.** as completed 2 years ago

James Valleroy mentioned in merge request !1899 (closed) 2 years ago

James Valleroy added In Review label and removed Next Release label 2 years ago

James Valleroy closed via commit 822c322d 2 years ago

James Valleroy mentioned in commit 822c322d 2 years ago

Please register or sign in to reply