miyagawa / **text.md**

Last active 11 years ago

Plack::Middleware::Session::Cookie vulnerability

text.md

Aug 11, 2014

Plack::Middleware::Session::Cookie 0.21 has a security vulnerability where it allows an attacker to execute arbitrary code on the server, when the middleware is enabled without a secret.

If you use Plack::Middleware::Session::Cookie, you're required to pass a `secret` option to the middleware. The value of the secret key must obviously be kept private.

- Version 0.22 is released today, which gives you a big WARNING when it is enabled without a secret set.
- Version 0.23 TRIAL is released, which refuses to run without a secret set, giving an error message on the startup. This will become a non-trial release in a few days.

Solution

- Set `secret` option to the middleware
- Use your own serializer/deserializer classes that are not Storable

Details

Because the middleware uses Storable module, an attacker could carefully craft a binary that could call DESTROY method on arbitrary classes (see `perldoc Storable` for SECURITY WARNING). Future versions of the middleware will change the default serialization method.

Thanks to mala (@bulkneets) for reporting this issue.