Pedro Fortuna, Co-Founder and CTO
Email: pedro.fortuna@jscrambler.com

Rua Alfredo Allen, 455
Ed Central UPTEC
Porto, Portugal 4200-135

FOR IMMEDIATE RELEASE: 09/09/2014

jscrambler
protect your code

Web Security Company JScrambler Announces the Release of JScrambler 3.6

Full-Stack JavaScript Source Code Protection

Porto, Portugal, September 9th, 2014 – Web security company JScrambler announces the release of JScrambler 3.6, the latest version of the HTML5/JavaScript protection service which now supports protecting the source code of Node.js applications.

With this new version, Node.js applications are now supported, making JScrambler a complete solution to protect anything with JavaScript. This release was fully tested with Node.js related libraries such as Express.js, Koa and Socket.io. Plus, it conveniently ships with a Node.js API client, and wrappers for Grunt and Gulp task runners.

This officially makes JScrambler 3.6 the first and only product in the market to protect JavaScript source code from the client to the server.

Node.js is not just for startups. PayPal, Yahoo and Microsoft are examples of bigger companies that are actively and openly using Node.js in their infrastructures. Expert JavaScript programmers are now able to program both the server and client side, which provides high efficiency, better quality and a lower cost of development.

Protecting Node.js code offers interesting solutions and explores new safety territories, the following are two of the scenarios of node.js application deployment:

1. Delivering Node.js code to others - companies develop applications for their clients and the codebase is customized and offered at competitive prices in order to boost the product development and adoption. Having exerted effort, time and money, firms sometimes are negligent regarding risk of the code being leaked to a third party. Competitors may inspect the code and become encouraged to create a copycat product. Clients may also hack the code, unlock features or simply pirate it. Hence, protecting the codebase makes sense by, for instance, obfuscating it and saving the IP legal disputes hassle.

2. Deploying Node.js apps to Cloud / Shared hosting - There are many advantages in using Cloud/shared Hosting. Yet uploading Web Apps on a virtual servers doesn't come without pitfalls, e.g. worrying about server outage, not knowing whether the security policies are strictly

followed or not, or risk hacking and illicit access. Hence by protecting the code, a extra layer of security is added, in case the code does end up in the hands of others they will not be able to re-use it.

“We tried other solutions & tools before choosing JScrambler. The level of protection combined with excellent support and frequent updates, is something we value very much.” Said Hannu Alakangas, CEO of Punos Mobile Ltd.

“With Node.js, where you are running your JavaScript is becoming a blur. Today you may be running it on the backend with Node.js, and tomorrow it is being shipped to the client device to be executed. This calls for a full stack JavaScript protection solution and JScrambler now claims to be it." He continued.

For developers interested in just minifying or compressing their JavaScript, they are encouraged to open a **https://jscrambler.com/en/** trial account. JScrambler offers this free of charge.

JScrambler has been around for almost four years, having so far protected around 150 million lines of JavaScript for users in more than 100 countries. JScrambler just got **Series A** funding in the beginning of this year and is now expanding its operations to the US.

Contact Information:

Pedro Fortuna, CTO

Email: pedro.fortuna@jscrambler.com

Mobile: +351 917 331 552

Twitter: @pedrofortuna - Skype: pedroffortuna

###