POLICY OF VULNERABILITY DISCLOSURE

1. General information information

We strive to ensure that expansion Posttrack (hereinafter - the "Application") for the Google browser Chrome, always It was protected and secure. When are identified vulnerability, we we put maximum effort into their elimination. AT Thisdocument describes our policy with regard of obtaining reports on potential vulnerabilities security our Applications, as well as standard practice to inform customers about proven vulnerabilities.

If you think that found vulnerability security in the Annex, we strongly we recommend that you inform us about th Nyo as can faster and do not publish vulnerability publicly as long as she will not fixed . we appreciate your help , and we We reviewall reports and do their best to in a timely manner decide similar problems . To encourage providing us with information about the vulnerability security , we will not apply to you with a suit in court if we define what disclosure information corresponds tothe following recommendations .

2. Guidance on Disclosure information

Notify and provide us with information about the vulnerability with the provision of time to eliminate vulnerability at least 1 (one month **)** before the public disclosure .

Provide appropriate level detailing vulnerability to we could identify and repr oduce the problem. Detailing vulnerability must include destination URLs, pairs request-response, screenshots and / or another information .

Attach reasonable efforts to to avoid service disruptions (e.g., DoS), problems privacy (for example, access to data User Posttrack) and destruction data during the research vulnerability .

Do not ask compensation for vulnerability reports security Applications.

Do not run automatic facilities Scan and send us the output, without confirming that the pr oblem is present. Instruments Security is often withdrawn false operation, which must be confirmed.

3. Categories vulnerabilities that we encourage

We are in the first place interesting learn about the following categories vulnerability :

- Cross -site scripting (XSS);
- CSRF;
- SQL Injection ;

- The problems associated with authentication;
- Questions relating to the authorization;
- Redirection attacks ;
- Remote performance code ;
- Unique issues that do not fall into the obvious category .

4. Categories vulnerabilities that we do not consider

The following categories vulnerabilities deal with beyond sphere our programs disclosure vulnerabilities :

- SSL Vulnerabilities associated with the configuration or version ;
- Denial of Service (DoS);
- Abuse function verification authenticity the user ;
- Brutus ;
- The HTTPOnly flag is not set to insensitive files cookie ;
- CSRF;
- Problems that are present only in old browsers / plugins ;
- The HTTP TRACE method is enabled;
- Reports on vulnerabilities associated with Web versions of servers, services, or frameworks ;
- Clickjacking on pages without authentication ;
- Reports about the vulnerabilities that require a large quantities interaction with the user to perform unlikely or unreasonable actions that were would more s uitable for social engineering or phishing attack, and not for application vulnerability (for example , shutdown functions browser protection , sending critically an important information an attacker to complete the attack by directing the user through a certain procedure and requiring that they themselves introduced a malicious code, etc.).

5. Changes in policy disclosure vulnerability

we We reserve the right to unilaterally order of change policies disclosure vulnerability, placing the relevant information on the site. therefore we ask you periodically check Availability changes .

6. Additional information

If you have questions on this policy or would like to discover more about politics disclosure vulnerability, send an email to our address posttrack@sloenka.com and we will get back to you.