

Multiple CRLF Injection / HTTP Response Splitting Vulnerabilities In Google AdWords

14th Dec, 2006

Vendor Name: Google

Product Name: Google AdWords (<https://adwords.google.com/>)

1. Descriptions:

Google AdWords is vulnerable to a new form of application attack technique called HTTP Response splitting (aka CRLF Injection). HTTP Response Splitting enables an attacker to alter the HTTP response header structure which can lead to wide range of attacks.

Although not limited to, it includes attacks such as web cache poisoning, temporary defacement, hijacking web pages or cross-site scripting (XSS). This happens since the user input is injected into the value section of HTTP header without properly escaping/removing CRLF characters which can lead to two HTTP responses instead of one response.

2. Affected Links:

GET /select/ProfessionalWelcome?hl=%0d%0afakeheader&null=Go HTTP/1.0

GET /select/Login?hl= hl=%0d%0afakeheader&null=Go HTTP/1.0

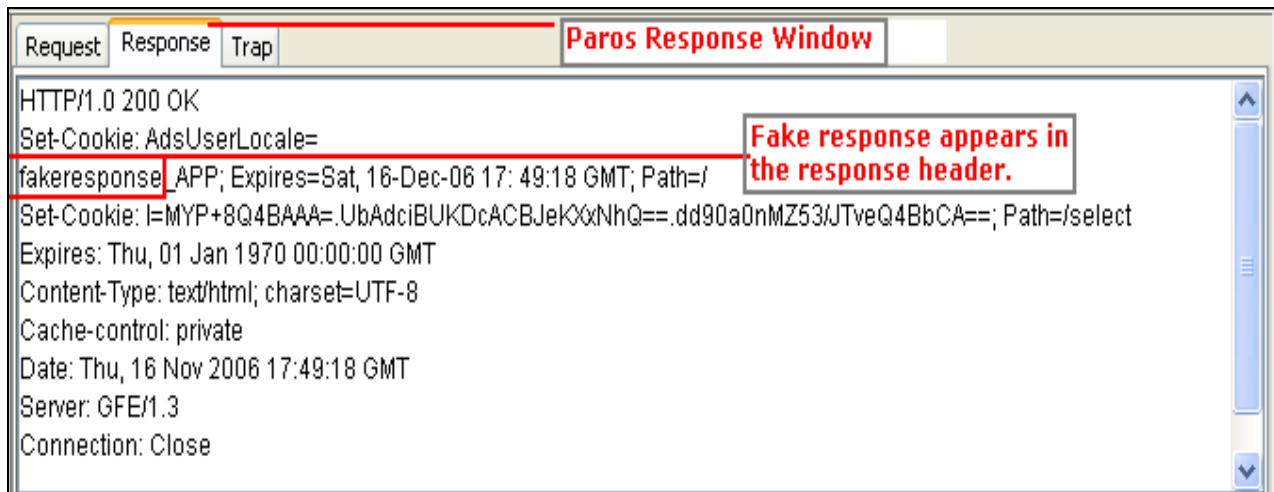
3. Proof-of-concept:

[Request Details]

Screenshot a: Custom HTTP response added to “hl” parameter

The screenshot shows a web browser window with the address bar containing the URL: `https://adwords.google.com/select/ProfessionalWelcome?hl=%0d%0afakeresponse&null=Go%20HTTP/1.0`. The page content includes the Google AdWords logo, the text "It's All About Results™", and a "Change Language" dropdown menu. A red box highlights the injected response in the URL, and another red box highlights the text "Fake response added to the parameter which will influence the response header." on the page. Below the logo, the text "Google Advertising Professionals" is displayed, followed by the tagline "Build your business. Get Google recognition. Make more money." and a paragraph of text: "Designed for professionals who currently manage or want to manage multiple AdWords client accounts, the Google A become a more successful ad manager – for free." There are two links: "Want to become a Google Advertising Professional?" and "Increase productivity with a more advanced AdWords" which leads to "My Client Center".

[Response Header]



4. Solution:

Sanitize CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom.

5. History:

11/20/2006 – Vendor Reported

11/20/2006 – Vendor replied back and asked for time to investigate

11/21/2006 – Vendor confirmed the report and asked for time to fix



11/21/2006 – Vendor replied saying, fix will be applied before 14th Dec

12/14/2006 – Public Disclosure

6. Credits:

Debasis Mohanty

d3basis.m0hanty@gmail.com