DefenseCode

DefenseCode ThunderScan SAST Advisory

google-api-php-client
Multiple Cross-Site Scripting (XSS) Vulnerabilities

google-api-php-client – Multiple Cross-Site Scripting (XSS) Vulnerabilities	
Advisory ID:	**DC-2017-04-012**
Software:	**google-api-php-client**
Software Language:	**PHP**
Version:	**2.1.3 and below**
Vendor Status:	**Vendor contacted, vulnerability confirmed**
Release Date:	**20170510**
Risk:	**Medium**

1. General Overview

During the security audit of google-api-php-client (Google's PHP client library for accessing Google APIs) multiple XSS vulnerabilities were discovered using DefenseCode ThunderScan SAST application source code security analysis platform.

More information about ThunderScan is available at URL:
http://www.defensecode.com

2. Software Overview

According to the API developers, the Google API Client Library enables you to work with Google APIs such as Google+, Drive, or YouTube on your server.

The developers further noted: "This client library is in beta. We will make an effort to support the library and maintain backwards compatibility in the future, but we reserve the right to make incompatible changes when necessary."

Homepage:
https://developers.google.com/api-client-library/php/
https://github.com/google/google-api-php-client

3. Vulnerability Description

During the security analysis, ThunderScan SAST discovered Cross Site Scripting vulnerability in Google's PHP client library for accessing Google APIs (google-api-php-client). The vulnerabilities were found in the sample code for using the Google's URL Shortener.

The Cross-Site Scripting vulnerability can enable the attacker to construct the URL that contains malicious JavaScript code. If the administrator of the site makes a request to such an URL, the attacker's code will be executed, with unrestricted access to the site in question. The attacker can entice the administrator to visit the URL in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum.

Once the unsuspecting user has visited such an URL, the attacker can proceed to send requests to the API on the behalf of the victim from his JavaScript.

3.1 Cross-Site Scripting	
Function:	**<?= $_SERVER['PHP_SELF'] ?>**
Variable:	**$_SERVER['PHP_SELF']**

Sample URL:

```
http://vulnerablesite.com/google-api-php-client/examples/url-shortener.php/%22%3E%3Cscript%3Ealert('xss')%3C/script%3E%3Cdc
```

File: google-api-php-client\examples\url-shortener.php

```
<form id="url" method="GET" action="<?= $_SERVER['PHP_SELF'] ?>">
```

3.2 Cross-Site Scripting	
Function:	**<?= $_SERVER['PHP_SELF'] ?>**
Variable:	**$_SERVER['PHP_SELF']**

Sample URL:

```
http://vulnerablesite.com/google-api-php-client/examples/url-shortener.php/%22%3E%3C/script%3E%3Cscript%3Ealert(42)%3C/script%3E?url=http%3A%2F%2Fwww.defensecode.com
```

File: google-api-php-client\examples\url-shortener.php

```
<a href="<?= $_SERVER['PHP_SELF'] ?>">Create another</a>
```

4. Solution

Vendor is expected to resolve security issues in the next release. All users are strongly advised to update google-api-php-client to the latest available version when the vulnerabilities get fixed.

5. Credits

Discovered by Leon Juranic with DefenseCode ThunderScan source code security analyzer.

6. Disclosure Timeline

2017/04/10	**Vendor contacted and fixes committed to GitHub as a merge request**
2017/04/10	**Automatic reply received instructing us to sign the CLA (Contributor License Agreement)**
2017/04/12	**CLA signed.**
2017/04/15	**Member of the Google Security Team responded: "*Nice catch!*"**
2017/04/21	**As part of Google's Vulnerability Reward Program, the panel has decided to issue us a financial reward.**
2017/05/10	**Advisory released to the public**

7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/