VASCO Security Response

Covert Redirect Flaw in OAuth does not affect MYDIGIPASS.COM

Response ID: vasco-sr-20140505-oauth

Revision number: 1.0

Date and time of release: May 5 2014 12:00 UTC

Date and time of last update: May 5 2014 12:00 UTC

Summary

Covert Redirect is a security flaw in the implementation of OAuth by Application Service Providers (ASPs), allowing attackers to obtain the personal data of users having an account with flawed ASPs. MYDIGIPASS.COM is safe from the Covert Redirect flaw.

What is OAuth?

OAuth is an open protocol for authorization. OAuth specifies a process to authorize third-party applications to obtain access to user accounts.

What is Covert Redirect?

Covert Redirect is a security flaw in the implementation of OAuth by Application Service Providers (ASPs), first published on 2 May 2014.

In the OAuth protocol, an ASP's website (e.g. example.com) makes an Authorization Request to the website of an authentication provider (e.g. mydigipass.com). This request contains an URI, such as https://ASP.com/redirect/?&original_page=https://ASP.com/myprofile. The authentication provider prompts the user to log into the authentication provider's domain, and then issues an Authorization Code to the ASP's website (example.com). This Authorization Code is passed from the authentication provider to the ASP's website by redirecting the user's browser to the URI provided in the Authorization Request.

The Covert Redirect flaw exists if ASPs allow an open redirect to a webpage chosen by an adversary. In this case an adversary would insert an URI redirecting to a rogue website into the Authorization Request, and the ASP would redirect to it. For instance, the URI https://example.com/redirect/?&original_page=https://evil.com/myprofile would cause a flawed ASP to redirect the user's browser to https://evil.com/myprofile, and this rogue website might subsequently access the user's personal data.

What is the impact of Covert Redirect?

Attackers can exploit the Covert Redirect security flaw to obtain the Authorization Code issued by the authentication provider. This Authorization Code may in turn be used to access account data of users stored by authentication providers. This data can subsequently be used for further malicious purposes.

Is MYDIGIPASS.COM vulnerable to Covert Redirect?

No, it is not.

MYDIGIPASS.COM performs two checks to ensure it is not subject to this flaw:

1. First, MYDIGIPASS.COM verifies whether the URI in the ASP's Authorization Request precisely matches the URI in MYDIGIPASS.COM's configuration settings for that ASP, in line with security recommendations of the IETF regarding OAuth. This not only ensures that MYDIGIPASS.COM redirects to the ASP's domain, but also that it redirects only to the specific webpage registered in MYDIGIPASS.COM by the ASP.
2. Second, MYDIGIPASS.COM authenticates the ASP when he requests an Access Token as part of an Authorization. The ASP has to provide its Client Secret to MYDIGIPASS.COM in order to authenticate itself. A rogue ASP would not be able to provide the Client Secret, which means it cannot access personal data of the MYDIGIPASS.COM users.

Legal disclaimer