10.16. 在隐式流程中滥用访问令牌假冒资源所有者(10. Access Token to Impersonate Resource Owner in Implicit Flow)

10.16. 在隐式流程中滥用访问令牌假冒资源所有者

对于使用隐式流程的公共客户端，本规范没有为客户端提供任何方法来决定访问令牌颁发给的是什么样的客户端。资源所有者可能通过给攻击者的恶意客户端许可访问令牌自愿委托资源的访问权限。这可能是由于钓鱼或一些其他借口。攻击者也可能通过其他机制窃取令牌。攻击者然后可能会尝试通过向合法公开客户端提供该访问令牌假冒资源拥

在隐式流程（response_type=token）中，攻击者可以轻易转换来自授权服务器的响应中的令牌，用事先颁发给攻击者的令牌替换真实的访问令牌。

依赖于在返回通道中传递访问令牌识别客户端用户的与本机应用程序通信的服务器可能由攻击者创建能够注入随意的窃取的访问令牌的危险的程序被类似地危及。任何做出只有资源所有者能够提交给它有效的为资源的访问令牌的假设的公共客户端都是易受这种类型的攻击的。这种类型的攻击可能在合法的客户端上泄露有关资源所有者的信息给攻击者（恶意客户端）。这也将允许攻击者在合法客户端上用和资源所有者相同的权限执行操作，该资源所有者最初许可了访问令牌或授权码。客户端对资源拥有者进行身份验证超出了本规范的范围。任何使用授权过程作为客户端对受委托的最终用户进行身份验证的形式的规范（例如，第三方登录服务）不能在没有其他的客户端能够判断访问令牌是否颁发是颁发给它使用的安

10.16. Misuse of Access Token to Impersonate Resource Owner in Implicit Flow

```
   For public clients using implicit flows, this specification does not   provide any method for the client to determine what client an access
   token was issued to.
   A resource owner may willingly delegate access to a resource by   granting an access token to an attacker's malicious client.  This may   be due to phishing or some other pretext.  An attacker may also steal
```

a token via some other mechanism. An attacker may then attempt to impersonate the resource owner by providing the access token to a

legitimate public client.

In the implicit flow (response_type=token), the attacker can easily switch the token in the response from the authorization server, replacing the real access token with the one previously issued to the

attacker.

Servers communicating with native applications that rely on being passed an access token in the back channel to identify the user of the client may be similarly compromised by an attacker creating a

compromised application that can inject arbitrary stolen access

tokens.

Any public client that makes the assumption that only the resource owner can present it with a valid access token for the resource is

vulnerable to this type of attack.

This type of attack may expose information about the resource owner at the legitimate client to the attacker (malicious client). This will also allow the attacker to perform operations at the legitimate client with the same permissions as the resource owner who originally

granted the access token or authorization code.

Authenticating resource owners to clients is out of scope for this specification. Any specification that uses the authorization process as a form of delegated end-user authentication to the client (e.g., third-party sign-in service) MUST NOT use the implicit flow without

additional security mechanisms that would enable the client to determine if the access token was issued for its use (e.g., audience-

restricting the access token).

Revision #1
Created Wed, Mar 25, 2020 11:29 PM by □□□
Updated Wed, Mar 25, 2020 11:30 PM by □□□