heimdall

security research

A DIVISION OF ISH

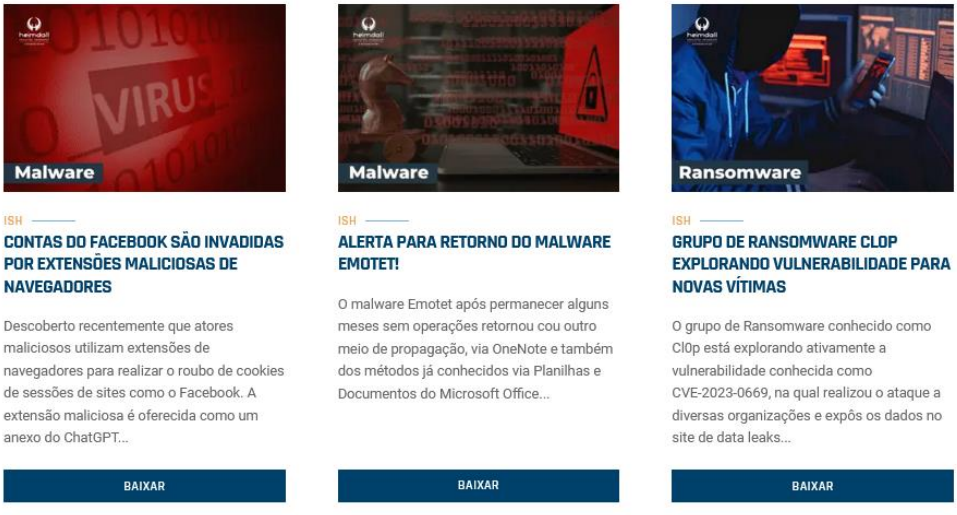
Configuração incorreta do Microsoft OAuth pode ocasionar escalação de privilégios no Azure AD

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 INTRODUÇÃO

O alerta a seguir, irá abordar um relatório publicado pela empresa Descope na qual identificaram que uma configuração incorreta nos aplicativos OAuth da Microsoft Azure AD ocasiona ao controle total da conta. Segundo a pesquisa, este tipo de problema foi apelidada como "nOAuth".

O nOAuth é uma falha da implementação de autenticação que pode afetar os aplicativos OAuth multiocatários do Microsoft Azure AD.

As especificações do OAuth, é de que o usuário é identificado pela declaração "sub" (assunto), sendo que a maioria dos IdPs fornece a declaração "e-mail" comum. Utilizar a declaração de e-mail como identificador de usuário poderá tornar um problema quando a declaração for mutável, logo é por isso que a maioria dos IdPs desaconselham a utilização de e-mail como identificador. No Microsoft Azure AD a declaração do e-mail é mutável e não verificada, portanto, nunca deve ser confiável ou utilizada como um identificador.

Neste caso, um ator malicioso pode alterar o atributo Email em "Informações de Contato" na conta do Azure AD para controlar a declaração "email" no JWT de identidade retornado.

Utilizando estas ações, poderá permitir que um invasor crie seu locatário do Azure AD use "Fazer login com a Microsoft" com um aplicativo vulnerável e um usuário "vítima" especialmente criado, resultando no controle total da conta.

O referido ataque foi relatado a Microsoft, a qual forneceu novas declarações para mitigar os casos em que o nOAuth é utilizado para falsificação entre locatários.

Para melhor entender a referida situação e vulnerabilidade do OAuth, iremos apresentar maiores detalhes nas seções a seguir.

2 CONEXÃO OAUTH E OPENID

O **Open Authorization (OAuth)** é uma estrutura de autorização aberta baseada em token que permite aos usuários conceder acesso a seus recursos privados em um aplicativo para outro aplicativo sem revelar seus detalhes de identidade. Por exemplo, um usuário do Facebook pode autorizar o Medium a acessar seu perfil, ler suas postagens ou postar em seu feed sem precisar fornecer ao Medium as suas credenciais do Facebook.

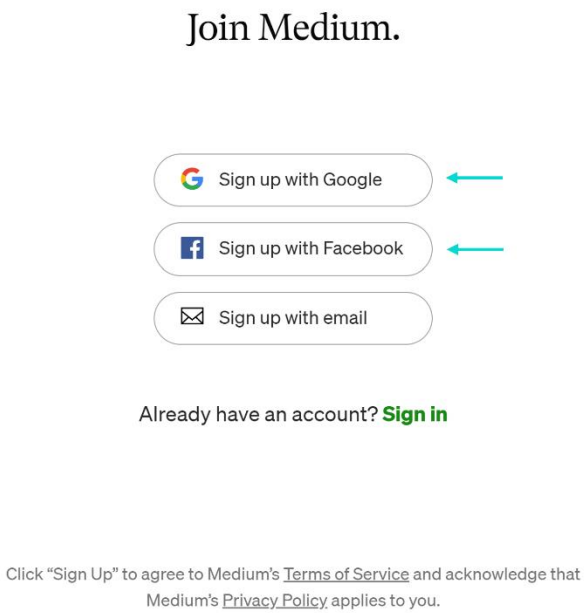


Figura 1 – OAuth para a página Medium.

O **OpenID Connected (OIDC)** é uma camada de identidade construída sobre OAuth 2.0 que permite que os aplicativos verifiquem as identidades dos usuários e obtenham informações básicas de perfil. O protocolo usa JSON Web Tokens (JWT) para transmitir com segurança essas informações entre as partes.

A combinação de ambos permite aos usuários realizar o login em sites utilizando a conta Microsoft, como exemplo.

3 Provedor de Identidade (IdP

Um **provedor de identidade (IdP)** é usado como uma fonte externa de verdade para identidades de usuários. Alguns dos provedores de identidades comuns são: Twitter, Facebook, Google, Okta e Azure AD.

4 Azure Active Directory (Azure AD)

O **Azure AD** é um serviço de gerenciamento de acesso e identidade baseado em nuvem. O Azure AD gerencia o acesso do usuário a recursos externos, como Microsoft365, portal Azure e outros aplicativos SaaS.

O Azure AD também gerencia recursos internos, como aplicativos em sua intranet corporativa e quaisquer aplicativos em nuvem desenvolvidos por sua própria organização, fornecendo autenticações via OAuth, OIDC e outros protocolos.

5 MESCLANDO CONTAS DE USUÁRIOS

Um grande exemplo que podemos utilizar, é quando o usuário acessa determinado site e ao realizar o login ou cadastro existe a possibilidade de "Faça o login com o Facebook" e "Faça o login com a Microsoft" como métodos de autenticação.

Neste caso, podemos supor que o usuário se cadastre com um link e utilize o serviço por um tempo e depois permanece inativo. Se o usuário retornar ao aplicativo, ele poderá esquecer qual o método de autenticação que utilizou para fazer login na última vez. Neste caso, poderá selecionar acidentalmente "Fazer login com a Microsoft".

Neste cenário, uma abordagem legal pode ser para o aplicativo identificar que o usuário que escolheu "Fazer login com a Microsoft" tem uma conta existente com base no endereço de e-mail fornecido pelo provedor de identidade e juntar as duas contas. Normalmente, isso poderia garantir a identidade do usuário seja unificada e que eles mantenham o controle sobre sua conta.

Porém, no nOAuth, como o endereço de e-mail não é confiável ou verificado, a fusão de contas de usuários resulta no controle total de conta pelo invasor.

6 CADEIA DE ATAQUE "NOAUTH"

Vamos imaginar um caso de ataque:

- Endereço de e-mail da vítima: **pesquisar@empresa[.]com**
- Endereço de e-mail do invasor: **malicioso@3331dfg.onmicrosoft.com**

Para que o invasor consiga explorar o **nOAuth**, ele seguirá a cadeia:

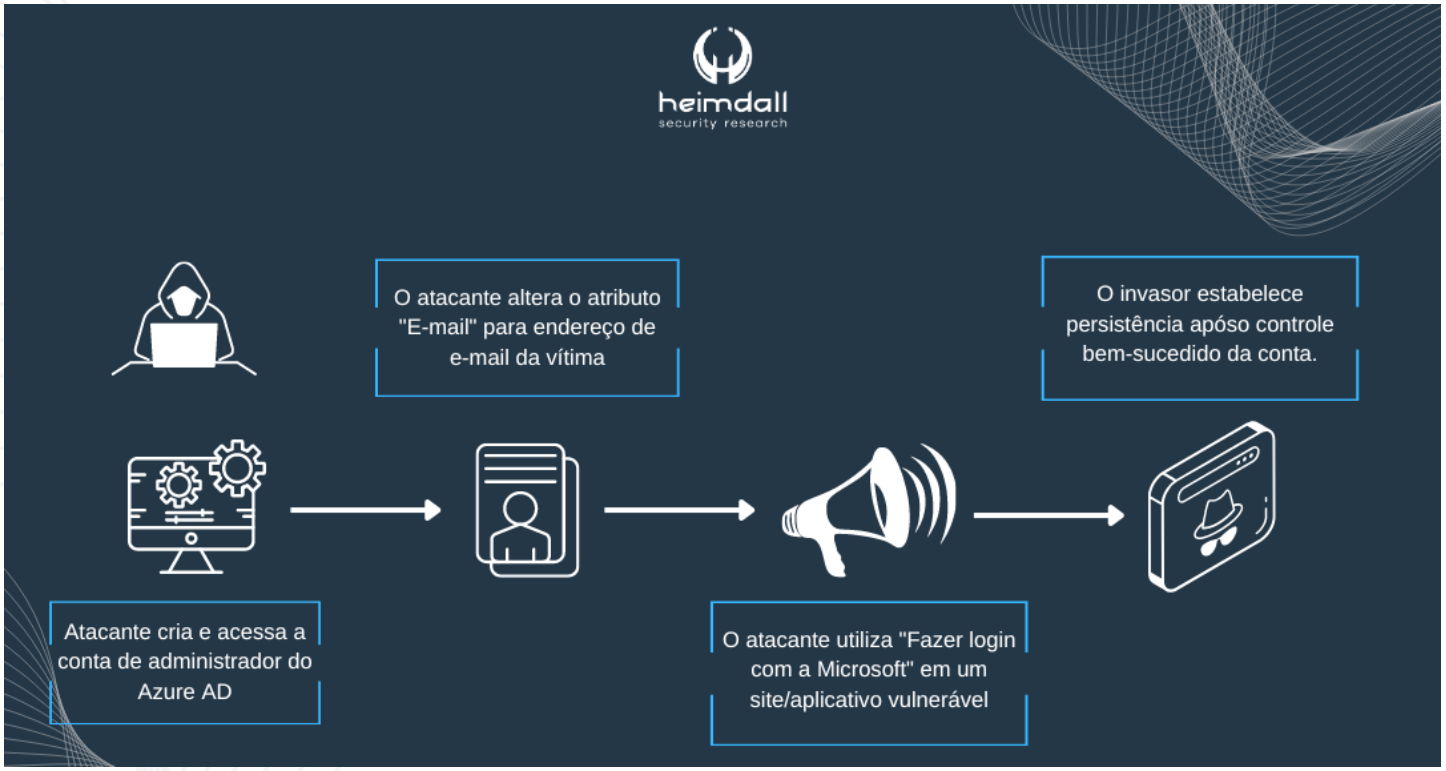


Figura 2 – Fluxo de ataque nOAuth.

Para a fase de **Preparar** o ataque, o ator malicioso irá realizar o acesso a conta que realizou a criação do Azure AD como administrador, na sequência irá alterar o atributo "E-mail" para o endereço de e-mail da vítima: **pesquisar@empresa[.]com** e, como a Microsoft acaba por não exigir que a alteração seja validada no Azure AD é apenas isto que o ator malicioso necessita fazer.

Já na fase de **Ataque**, o ator malicioso irá utilizar a opção "Fazer login com a Microsoft" em um site/aplicativo vulnerável a nOAuth (ou seja, um que utiliza o endereço de e-mail como um identificador exclusivo). Caso o aplicativo ou site mescle as contas de usuário sem realizar

validação, o invasor terá controle total sobre a conta da vítima, mesmo que ela não tenha uma conta da Microsoft.

Após o login bem-sucedido, o invasor tem um campo aberto, dependendo da natureza do aplicativo ou site que assumiu. Logo, os atores podem realizar a persistência, exfiltrar dados, explorar outros dispositivos por meio de movimento lateral e outros.

A captura de tela realizada pela Descope, é possível perceber dois logins 0Auth diferentes para o mesmo aplicativo, podendo ser observado que todos os valores são os mesmos, apenas o valor "E-mail" são diferentes.

Figura 3 – Métodos distintos de validação através do e-mail.

A Descope publicou também um vídeo demonstrando a cadeia de ataque através do nOAuth.

7 O QUE DISSE A MICROSOFT

A Microsoft foi informada acerca da referida vulnerabilidade, sendo que dias após realizar a comunicação com a Microsoft, esta publicou em uma página dedicada à validação de declarações todas as informações que um desenvolvedor precisa considerar ao implantar a autenticação.

Os desenvolvedores podem utilizar duas novas declarações para ajudar a evitar que o nOAuth seja utilizado em aplicativo:

- **xms_edov [Email Domaion Owner Verified]:** a qual é uma declaração opcional que indica se uma declaração de e-mail contém um endereço de e-mail verificado pelo domínio.
- **RemoveUnverifiedEmailClaim:** é um sinalizador de comportamento de autenticação que pode redigir declarações de e-mail quando o domínio do e-mail não é verificado.

Os demais detalhes poderão ser buscados através da publicação da Microsoft sobre o tema.

8 APLICATIVOS VULNERÁVEIS

Segundo a Descobe, diversos sites e aplicativos foram testados para fins de identificar quais estavam sendo vulneráveis a este tipo de ataque, sendo que, foram obtidas informações relevantes de muitos destes aplicativos e sites estavam vulneráveis.

Lembrando que a recomendação é que se caso o aplicativo/site estiver utilizando o "Fazer login com a Microsoft", recomendamos verificar imediatamente se ele é vulnerável ao "nOAuth" e corrigi-lo.

Logo, existem dois cenários para aplicativos que utilizam provedor de autenticação de terceiros que podem ocorrer após uma tentativa de "Fazer login com a Microsoft" para um usuário que já possui uma conta anterior da Microsoft vinculada:

- As duas contas são mescladas
- As duas contas não são mescladas

Para a etapa de correção, a Microsoft sugeriu na publicação sobre documentação de validação de declarações que o **"upc", "email", "preferred_username"** e outros tipos de valores não devem ser utilizadas para tomar decisões de autenticação ou autorização.

Logo, é de extrema importância a validação caso haja a utilização de validação por parte de aplicativos/sites que utilizem apenas o atributo de e-mail como validador para a autenticação ou autorização, podendo ocasionar incidentes de seguranças e também outros tipos de ataques por atores maliciosos.

9 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Pesquisa e relatório Descope - nOAuth**
- **Recomendações Microsoft para criar métodos de autenticação.**
- **Medidas e recomendações para autenticação com APIs - Microsoft**
- **Potencial risco de escalonamento de privilégios em aplicativos do Azure – Microsoft.**

heimdall
security research

A DIVISION OF ISH