Falha no ID do Microsoft Entra permitiu sequestrar o inquilino de qualquer

Data: 2025-09-21 17:32:06

Autor: Inteligência Against Invaders

Uma combinação crítica de componentes herdados poderia ter permitido acesso completo ao

locatário do Microsoft Entra ID de todas as empresas do mundo.

A combinação fatal incluiu tokens não documentados chamados “tokens de ator” e uma vulnerabilidade na API do Azure AD Graph (CVE-2025-55241) que permitia que os tokens funcionassem com o ambiente de ID do Entra de qualquer organização.

Um agente de ameaça que explorasse o problema teria acesso a uma série de dados altamente confidenciais sem deixar rastros nos logs do ambiente de destino, exceto por suas próprias ações.

O Entra ID é o serviço de gerenciamento de identidade e acesso (IAM) baseado em nuvem da Microsoft, anteriormente conhecido como Azure Active Directory (Azure AD), que fornece às organizações logon único, autenticação multifator e controles de segurança em aplicativos e recursos.

Uma instância dedicada do Entra ID representa uma única organização e gerencia o acesso seguro a todos os aplicativos usados, tanto no local quanto na nuvem.

Isso pode incluir serviços do Microsoft 365, produtos SaaS personalizados e de terceiros, como Salesforce, Dropbox ou aplicativos de nuvem do Google, Amazon ou SAP.

Pesquisador de segurança Dirk-jan Mollema, fundador da segurança ofensivaSegurança externa, descobriu uma falha de validação de token que lhe dava privilégios de administrador global em todos os locatários do Entra ID.

Esse nível de acesso permite o comprometimento total do locatário e abre a porta para qualquer serviço autenticado por meio do Entra ID.

Representando qualquer usuário no locatário

Em uma postagem técnica no blog, Mollema explica que os tokens de ator são emitidos por um serviço legado chamado Access Control Service, que “é usado para autenticação com aplicativos do SharePoint e também parece ser usado pela Microsoft internamente”.

O pesquisador os encontrou enquanto investigava configurações híbridas do Exchange. Ele notou que o Exchange os solicitava ao se comunicar com outros serviços em nome de um usuário.

“O token de ator permite que ele ‘atue’ como outro usuário no locatário ao se comunicar com o Exchange Online, o SharePoint e, como se vê, o Azure AD Graph” – Dirk-jan Mollema

Os tokens de ator não são assinados, o que significa que podem ser usados para representar qualquer usuário no locatário e têm validade de 24 horas sem a possibilidade de serem revogados durante esse período.

Mollema diz que “todo esse design de token de ator é algo que nunca deveria ter existido”, porque eles não têm os controles de segurança necessários adequados:

- não há logs quando os tokens de ator são emitidos
- como esses serviços podem criar os tokens de representação não assinados sem se comunicar com o ID do Entra, também não há logs quando eles são criados ou usados
- eles não podem ser revogados dentro de sua validade de 24 horas
- eles ignoram completamente todas as restrições configuradas no Acesso Condicional
- Temos que confiar no registro do provedor de recursos para saber que esses tokens foram usados no locatário

O pesquisador diz que a Microsoft depende de tokens de ator internamente para comunicação serviço a serviço e que a empresa planeja removê-los.

A Microsoft os chama de “acesso com privilégios elevados (HPA)” que permite que um aplicativo ou serviço “se passe por outros usuários sem fornecer qualquer prova do contexto do usuário.

Ao testar várias maneiras de usar um token de ator, Mollema alterou a ID do locatário para uma diferente daquela que gerou o token e a enviou para a API do Graph do Azure AD preterida (graph.windows.net), esperando uma mensagem de “acesso negado”.

Em vez disso, o erro que o pesquisador viu indicou que o token era válido, mas o acesso não foi autorizado porque a identidade do usuário não foi encontrada no locatário.

[IMAGEM REMOVIDA]Administrador global no locatário de destino e executar todas as ações associadas à função (por exemplo, gerenciar e criar usuários de diferentes funções, modificar configurações, redefinir senhas, adicionar administradores).

Mollema destaca que nenhuma das ações necessárias para obter privilégios de administrador global gerou logs no locatário da vítima.

Do ponto de vista de um invasor, explorar os problemas teria sido possível em algumas etapas, começando com a geração do token de ator de um locatário sob seu controle:

- Encontrar a ID do locatário para o ambiente de destino pode ser feito com APIs públicas com base no nome de domínio
- Localizando um netId válido de um usuário regular no locatário de destino
- Criando uma personificaçãoion token com o token de ator do locatário invasor usando o ID do locatário e *netId* do usuário no locatário vítima
- Listando todos os Administradores Globais no locatário e seus *netId*
- Criar um token de representação para o administrador global
- Executando qualquer ação de leitura/gravação por meio da API do Graph do Azure AD

Mollema observa que apenas a atividade na última etapa seria registrada no inquilino vítima.

É importante observar que a Microsoft iniciou o processo de substituição do serviço Azure AD Graph API em setembro do ano passado.

No final de junho, a empresa alertou que os aplicativos configurados para Acesso estendido mas ainda usava o Azure AD Graph, não seria mais capaz de usar as APIs a partir do início de setembro de 2025.

Mollema relatou os problemas à Microsoft em 14 de julho e a empresa confirmou que o problema foi resolvido nove dias depois.

Em 4 de setembro, a Microsoft também CVE-2025-55241 corrigido, descrevendo-o como uma vulnerabilidade crítica de escalonamento de privilégios no Azure Entra.

[IMAGEM REMOVIDA]