BOLETIM DE SEGURANÇA

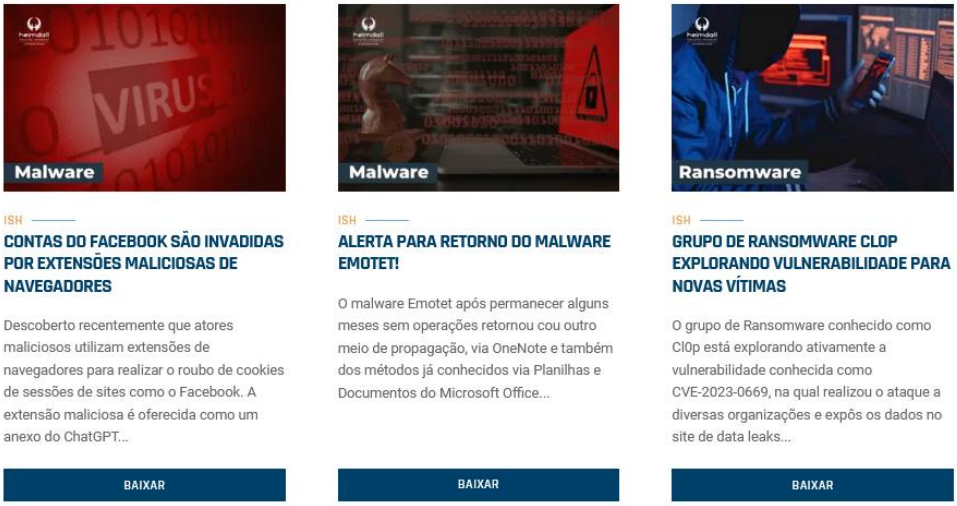
Falhas em aplicativos Microsoft para macOS expõem usuários a riscos de acesso irrestrito

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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

Boletins de Segurança – Heimdall



SUMÁRIO

1 Sumário Executivo 5
2 Informações sobre a ameaça 6
3 Recomendações 11
4 Referências 12
5 Autores 13

LISTA DE FIGURAS

Figura 1 – Exemplo de prompt de permissão para Malevolent App. 7
Figura 2 – Duplicações de permissões. 8
Figura 3 – Injeção cd biblioteca maliciosa. 8
Figura 4 – Fluxo simples que verifica se um aplicativo é potencialmente vulnerável à injeção de biblioteca. 9

1 SUMÁRIO EXECUTIVO

A Cisco identificou oito vulnerabilidades em aplicativos da Microsoft no sistema macOS, permitindo que um atacante obtenha acesso a dados confidenciais ou eleve privilégios sem o consentimento do usuário. Essas falhas exploram brechas no modelo de segurança baseado em permissões do macOS, conhecido como Transparência, Consentimento e Controle (TCC), o que possibilita contornar as barreiras impostas pelo sistema operacional.

2 INFORMAÇÕES SOBRE A AMEAÇA

Essas vulnerabilidades, um invasor pode realizar ações como enviar e-mails em nome do usuário ou capturar fotos e vídeos sem interação. A Microsoft considerou essas falhas de baixo risco e, em alguns casos, optou por não corrigi-las, alegando que a execução de bibliotecas não assinadas é necessária para suportar certos plug-ins. Abaixo segue a lista detalhada das vulnerabilidades, incluindo seus respectivos CVEs e Ids.

A CVE-2024-42220, corresponde a uma vulnerabilidade de injeção de biblioteca no Microsoft Outlook 16.83.3 para macOS. Uma biblioteca desenvolvida especialmente pode tirar proveito dos privilégios de acesso do Outlook, resultando em um desvio de permissões. Um aplicativo mal-intencionado pode injetar uma biblioteca e executar o programa para explorar essa falha, aproveitando os privilégios do aplicativo comprometido. A Talos verificou, ou o fornecedor confirmou, que a versão 16.83.3 do Microsoft Outlook para macOS é vulnerável.

A CVE-2024-42004, descreve uma vulnerabilidade de injeção de biblioteca no Microsoft Teams (work or school), versão 24046.2813.2770.1094 para macOS. Assim como no caso anterior, uma biblioteca criada para esse propósito pode explorar os privilégios de acesso do Teams, provocando um desvio de permissões. Um aplicativo malicioso pode injetar essa biblioteca, lançar o programa e explorar a vulnerabilidade, utilizando os privilégios do Teams. A versão mencionada foi testada e confirmada como vulnerável pela Talos ou pelo fornecedor.

A CVE-2024-39804, refere-se a uma vulnerabilidade de injeção de biblioteca no Microsoft PowerPoint 16.83 para macOS. Uma biblioteca especialmente construída pode explorar os privilégios do PowerPoint, resultando em um desvio de permissões. Um aplicativo mal-intencionado pode injetar essa biblioteca e iniciar o programa para explorar a falha. A versão 16.83 do Microsoft PowerPoint para macOS foi identificada como vulnerável pela Talos ou confirmada pelo fornecedor.

A CVE-2024-41159, trata de uma vulnerabilidade semelhante no Microsoft OneNote 16.83 para macOS. Uma biblioteca maliciosa pode ser injetada para obter controle dos privilégios de acesso do OneNote, permitindo um desvio de permissão. Um aplicativo malicioso pode injetar essa biblioteca, iniciar o programa e aproveitar a falha de segurança. A Talos verificou essa vulnerabilidade ou ela foi confirmada pelo fornecedor.

A CVE-2024-43106, é uma falha de injeção de biblioteca no Microsoft Excel 16.83 para macOS. Uma biblioteca especialmente criada pode se aproveitar dos privilégios do Excel, provocando um desvio de permissões. Aplicativos maliciosos podem injetar essa biblioteca para explorar a falha ao iniciar o Excel. As versões vulneráveis foram testadas ou confirmadas pela Talos ou pelo fornecedor.

A CVE-2024-41165, é uma vulnerabilidade de injeção de biblioteca no Microsoft Word 16.83 para macOS. Uma biblioteca maliciosa pode explorar os

privilégios do Word, causando um desvio de permissões. Um aplicativo mal-intencionado pode injetar a biblioteca e iniciar o Word, explorando a falha de segurança. As versões vulneráveis foram testadas ou confirmadas como vulneráveis pela Talos ou pelo fornecedor.

A CVE-2024-41145, envolve uma vulnerabilidade no aplicativo auxiliar WebView.app do Microsoft Teams (work or school) 24046.2813.2770.1094 para macOS. Uma biblioteca especialmente construída pode tirar vantagem dos privilégios de acesso do Teams, provocando um desvio de permissões. Um aplicativo malicioso pode explorar essa falha por meio da injeção de uma biblioteca e inicialização do programa. A Talos testou ou o fornecedor confirmou a vulnerabilidade nessas versões.

A CVE-2024-41138, refere-se a uma falha no aplicativo auxiliar com.microsoft.teams2.modulehost.app do Microsoft Teams (work or school) 24046.2813.2770.1094 para macOS. Semelhante às outras, uma biblioteca maliciosa pode ser injetada para explorar os privilégios de acesso, resultando em um desvio de permissões. As versões vulneráveis foram testadas pela Talos ou confirmadas pelo fornecedor.

A política de segurança da maioria dos sistemas operacionais é baseada, em geral, no Discretionary Access Control (DAC), que oferece proteção básica contra softwares maliciosos ou ataques que operam com privilégios de usuário ou root. O macOS da Apple, no entanto, vai além disso ao incluir camadas extras de proteção, como o TCC, que regula como os aplicativos acessam dados confidenciais dos usuários e recursos do sistema. O TCC impõe que os aplicativos obtenham consentimento explícito do usuário para acessar informações sensíveis, como contatos, fotos, localização e calendário, assegurando que os usuários tenham controle total sobre seus dados. Além disso, os desenvolvedores de aplicativos precisam solicitar permissões específicas através de "direitos", que são capacidades fornecidas pela Apple para regular o acesso aos recursos.

Quando um aplicativo solicita permissão para usar um recurso protegido, como a câmera, uma janela pop-up é exibida pedindo a aprovação do usuário. Caso o usuário permita ou negue o acesso, essa decisão é armazenada no banco de dados do TCC e será aplicada a futuros acessos desse aplicativo ao mesmo recurso.

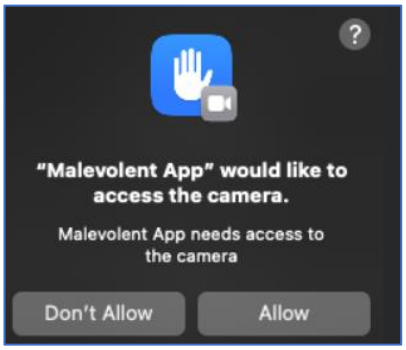


Figura 1 – Exemplo de prompt de permissão para Malevolent App.

Essas permissões podem ser verificadas e gerenciadas posteriormente na seção "**Privacy & Security**" do macOS, onde o usuário pode visualizar e ajustar as permissões de aplicativos para a câmera, microfone e serviços de localização. Outro mecanismo importante do macOS é o sandbox, obrigatório para aplicativos da Mac App Store. O sandbox limita o acesso dos aplicativos aos recursos do sistema, garantindo que eles só acessem o que foi explicitamente autorizado pelos direitos solicitados. Para algumas funcionalidades, como acesso à câmera, o uso de sandbox pode gerar novas solicitações de permissão ao usuário, conforme exigido pelo TCC.

Os recursos de sandbox e runtime reforçado podem ser combinados para aumentar a proteção. Em alguns casos, isso pode resultar em uma aparente duplicação de permissões. Por exemplo, quando um aplicativo utiliza tanto o sandbox quanto o runtime reforçado e precisa acessar o microfone, ele terá duas permissões diferentes: uma referente ao sandbox e outra ao runtime reforçado.

```
com.apple.security.device.audio-input
com.apple.security.device.microphone
```

Figura 2 – Duplicações de permissões.

A campanha de pesquisa realizada tem como foco principal a capacidade de injetar uma biblioteca e explorar as permissões ou privilégios de outros aplicativos. A técnica de injeção de biblioteca, chamada **Dylib Hijacking** no macOS, envolve a inserção de código no processo em execução de um aplicativo. O macOS protege contra essa ameaça com medidas como o tempo de execução reforçado, que diminui a chance de um atacante executar código arbitrário no processo de outro aplicativo. Contudo, se um invasor injetar uma biblioteca no processo ativo de um aplicativo, essa biblioteca pode usar todas as permissões já atribuídas ao processo, atuando em nome do aplicativo.

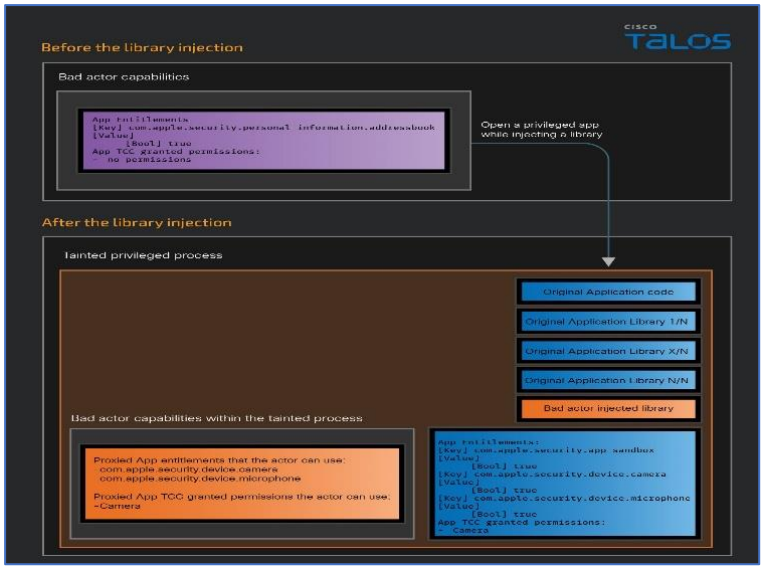


Figura 3 – Injeção cd biblioteca maliciosa.

O macOS da Apple possui um modelo de segurança em camadas, incluindo o TCC e direitos, que visam garantir a privacidade dos usuários e a segurança do sistema. O TCC controla o acesso dos aplicativos a dados pessoais e privilégios do sistema, exigindo aprovação explícita do usuário para liberar esse acesso. Apesar de sua robustez, o modelo de segurança do macOS não é infalível. Permissões elevadas concedidas a aplicativos podem ser exploradas, transformando esses programas em pontos de entrada para acessos não autorizados a dados sensíveis. A eficácia do TCC depende de como os aplicativos gerenciam suas permissões. Se um aplicativo confiável for comprometido, ele pode ser usado para abusar de seus privilégios, permitindo que invasores executem ações sem o conhecimento do usuário. Um exemplo seria um aplicativo de vídeo que, explorado, pode gravar sem alertar o usuário. Isso revela um ponto crucial: o macOS depende de que os aplicativos administrem bem suas permissões. Uma falha nesse processo pode comprometer todo o modelo de permissão, permitindo que aplicativos atuem como proxies para acessos não autorizados, contornando o TCC e ameaçando a segurança do sistema. Isso reforça a necessidade de medidas de segurança robustas nos aplicativos para evitar que sejam explorados.

As vulnerabilidades em questão surgem quando um aplicativo carrega bibliotecas de locais que podem ser manipulados por um invasor. Se o aplicativo tiver o direito **com.apple.security.cs.disable-library-validation**, ele permite que um invasor injete qualquer biblioteca e execute código arbitrário no aplicativo comprometido, explorando assim todas as permissões e direitos do mesmo.

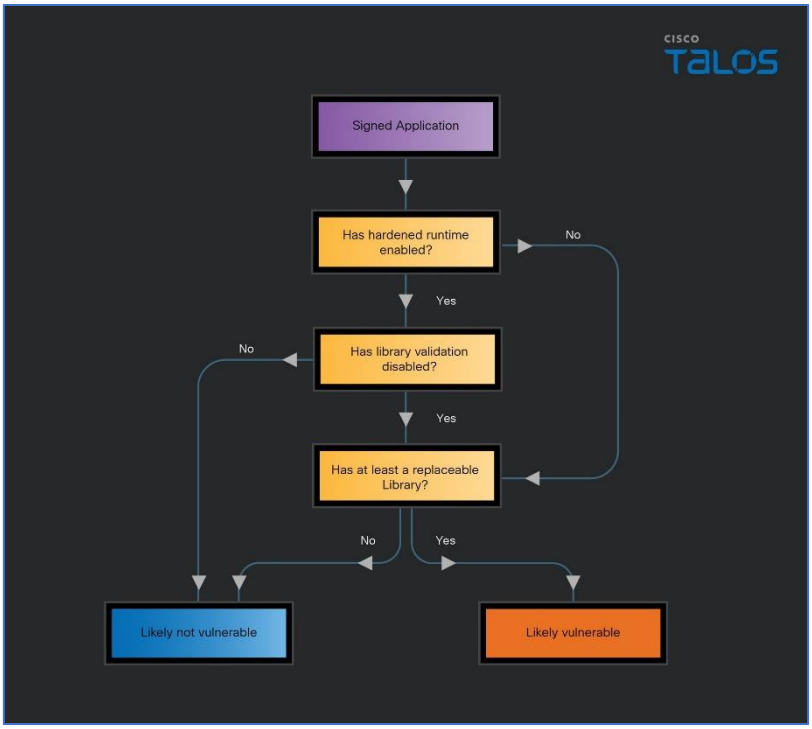


Figura 4 – Fluxo simples que verifica se um aplicativo é potencialmente vulnerável à injeção de biblioteca.

O modelo de segurança do macOS oferece proteção aprimorada em relação aos sistemas de política DAC tradicionais. Ele notifica os usuários quando um aplicativo tenta acessar dados confidenciais ou recursos de privacidade e inclui mecanismos que impedem a injeção dinâmica de bibliotecas, neutralizando uma série de vulnerabilidades. Embora novas falhas possam surgir, esse sistema reduz os riscos e aumenta a conscientização dos usuários. Embora a Microsoft considere o risco baixo, quatro dos oito aplicativos relatados foram atualizados e não possuem mais esse direito, eliminando a vulnerabilidade:

- Microsoft Teams (aplicativo principal)
- Microsoft Teams WebView.app
- Microsoft Teams ModuleHost.app (antes com.microsoft.teams2.modulehost.app)
- Microsoft OneNote

No entanto, os seguintes aplicativos ainda estão vulneráveis:

- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Word

Esses aplicativos continuam permitindo que invasores reutilizem as permissões sem interação do usuário, atuando como um canal para ações maliciosas. A Microsoft parece utilizar o direito para permitir "plug-ins", que, no caso, são complementos baseados na web conhecidos como "Office add-ins".

3 RECOMENDAÇÕES

Abaixo seguem as recomendações de segurança necessárias:

- **CVE-2024-42220**: Atualize para a versão mais recente do Microsoft Outlook para macOS e evite a execução de aplicativos não confiáveis.
- **CVE-2024-42004**: Atualize para a versão mais recente do Microsoft Teams (work or school) para macOS e evite executar bibliotecas não assinadas.
- **CVE-2024-39804**: Atualize para a versão mais recente do Microsoft PowerPoint para macOS e evite a execução de bibliotecas não confiáveis.
- **CVE-2024-41159**: Atualize para a versão mais recente do Microsoft OneNote para macOS e evite a execução de bibliotecas não assinadas.
- **CVE-2024-43106**: Atualize para a versão mais recente do Microsoft Excel para macOS e evite a execução de bibliotecas não confiáveis.
- **CVE-2024-41165**: Atualize para a versão mais recente do Microsoft Word para macOS e evite a execução de bibliotecas não assinadas.
- **CVE-2024-41145**: Atualize para a versão mais recente do aplicativo auxiliar WebView do Microsoft Teams (work or school) para macOS e evite a execução de bibliotecas não confiáveis.
- **CVE-2024-41138**: Atualize para a versão mais recente do aplicativo auxiliar com.microsoft.teams2.modulehost.app do Microsoft Teams (work or school) para macOS e evite a execução de bibliotecas não assinadas.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Talos
- Thehackernews
- NVD

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH