



BOLETIM DE SEGURANÇA

Vulnerabilidades no Microsoft Account e Azure AI Face Service expõem sistemas a elevação de privilégios

Acesse a nossa nova comunidade através do
WhatsApp!

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



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como ClOp está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

| | | |
|-----|--|---|
| 1 | Introdução executiva..... | 4 |
| 2 | Informações sobre as vulnerabilidades..... | 5 |
| 2.1 | Sistemas e produtos afetados | 5 |
| 2.2 | Impacto da vulnerabilidade | 5 |
| 3 | Recomendações..... | 6 |
| 4 | Referências | 7 |
| 5 | Autores..... | 7 |

1 INTRODUÇÃO EXECUTIVA

A Microsoft divulgou duas vulnerabilidades importantes em seus alertas: **CVE-2025-21396** e **CVE-2025-21415**. A primeira afeta o **Microsoft Account**, permitindo que um atacante não autorizado eleve privilégios através da rede. A segunda impacta o **Azure AI Face Service**, possibilitando que um atacante autorizado eleve seus privilégios por meio de uma falha de autenticação.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Segue abaixo, as vulnerabilidades informadas pela Microsoft, juntamente com uma breve descrição de cada uma:

[CVE-2025-21396](#)

- Esta vulnerabilidade decorre de uma falha de autorização no Microsoft Account, permitindo que um atacante não autorizado eleve seus privilégios através da rede. A falha está associada à ausência de verificações adequadas de autorização, classificando-a sob a [CWE-862](#): "Falta de Autorização". Um atacante pode explorar essa vulnerabilidade enviando solicitações especialmente criadas para contornar os mecanismos de autorização, obtendo acesso a funcionalidades ou dados que normalmente requerem privilégios elevados.

[CVE-2025-21415](#)

- Esta vulnerabilidade está presente no Azure AI Face Service e permite que um atacante autorizado eleve seus privilégios através da rede. A falha está relacionada a um bypass de autenticação por meio de spoofing, permitindo que o atacante obtenha privilégios elevados no serviço. Um atacante pode explorar essa vulnerabilidade manipulando o processo de autenticação para obter privilégios adicionais, potencialmente acessando ou modificando dados sensíveis.

2.1 SISTEMAS E PRODUTOS AFETADOS

A vulnerabilidade afeta as seguintes ferramentas:

CVE-2025-21396

- Microsoft Account

CVE-2025-21415

- Azure AI Face Service

2.2 IMPACTO DA VULNERABILIDADE

Os impactos das vulnerabilidades identificadas nos produtos da Microsoft incluem:

- Acesso não autorizado
- Escalação de privilégios
- Comprometimento de dados sensíveis
- Comprometimento de autenticação
- Interrupção de serviços

3 RECOMENDAÇÕES

Para mitigar os riscos associados às vulnerabilidades identificadas nos produtos da Microsoft, recomenda-se:

Aplicar atualizações

- A Microsoft já implementou medidas para mitigar ambas as vulnerabilidades. Recomenda-se que os usuários e administradores garantam que seus sistemas estejam atualizados com as últimas correções fornecidas pela Microsoft.

Monitoramento contínuo

- Implementar monitoramento contínuo dos sistemas para detectar atividades suspeitas ou tentativas de exploração dessas vulnerabilidades.

Revisão de políticas de acesso

- Revisar e reforçar as políticas de acesso e autenticação, garantindo que apenas usuários autorizados tenham acesso aos recursos críticos e que mecanismos de autenticação robustos estejam em vigor.

4 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Microsoft](#)
- [CWE](#)
- [The Hacker News](#)

5 AUTORES

- Rafael Salomé



heimdall
security research

A DIVISION OF ISH