BOLETIM DE SEGURANÇA

Falha de segurança no Wi-Fi facilita interceptação de dados através de ataques de downgrade

heimdall
security research
A DIVISION OF ISH

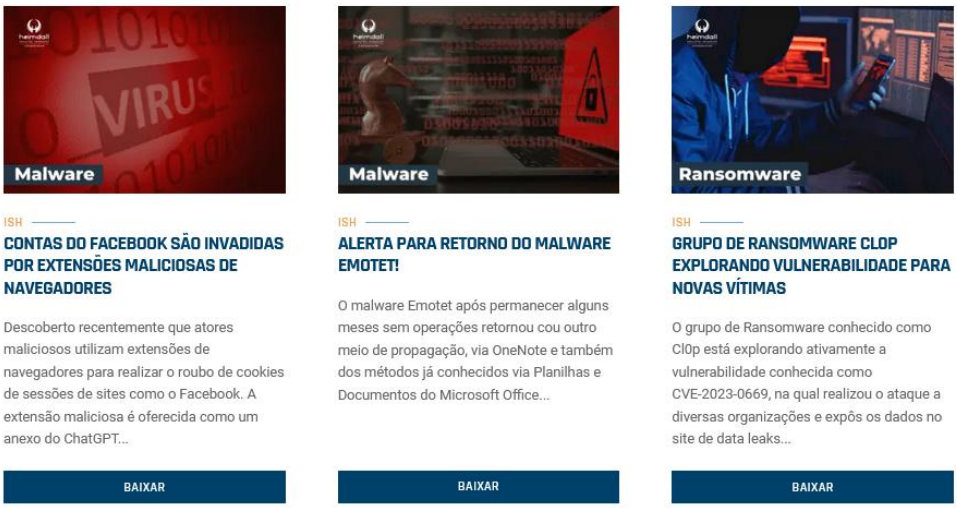
TLP: CLEAR

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

[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

1 Sumário Executivo 5
2 Informação sobre a ameaça 6
3 Recomendações 8
4 Referências 9
5 Autores 10

LISTA DE FIGURAS

Figura 1 – Categoria de redes Wi_Fi. *6*

Figura 2 – Detalhes do ataque de SSID Confusion. *7*

1 SUMÁRIO EXECUTIVO

Pesquisadores identificaram uma vulnerabilidade CVE-2023-52424 categorizada como crítica, onde permite que atacantes induzam as vítimas a se conectar a uma versão mais vulnerável da rede sem fio, possibilitando a espionagem do tráfego de dados.

2 INFORMAÇÃO SOBRE A AMEAÇA

A vulnerabilidade CVE-2023-52424, conhecido como ataque de "SSID Confusion", impacta uma gama de sistemas operacionais e dispositivos que utilizam Wi-Fi, abrangendo tanto redes domésticas quanto redes mesh que operam com os protocolos WEP, WPA3, 802.11X/EAP e AMPE. Ela permite que atacantes criem redes falsas com SSIDs enganosos, atraindo vítimas que reutilizam credenciais, expondo-as a riscos de interceptação e alteração de dados. Além disso, VPNs que se desativam automaticamente em redes “confiáveis” podem ser desligadas inadvertidamente. Até o momento, seis universidades, incluindo no Reino Unido e EUA, foram identificadas como locais de alto risco para funcionários e estudantes devido à prática de reutilizar credenciais.

A causa raiz está no protocolo IEEE 802.11, que é a base do funcionamento do Wi-Fi, residindo na ausência de um mecanismo obrigatório de autenticação para o SSID da rede. Os dispositivos que buscam redes Wi-Fi nos quadros de beacon emitidos pelos pontos de acesso, que contêm o SSID, sem realizar uma autenticação. Essa busca inerente é explorada pelos atacantes, que estabelecem redes com SSIDs fraudulentos, induzindo os dispositivos a se conectarem a elas. A suposição equivocada de que a segurança é necessária apenas no momento da conexão com a rede é a raiz dessa vulnerabilidade, tornando todos os dispositivos Wi-Fi suscetíveis ao ataque de SSID Confusion. Os testes demonstraram que, sob as condições certas, qualquer dispositivo pode ser comprometido por esse tipo de ataque.

A Imagem abaixo categoriza as redes Wi-Fi e seus respectivos protocolos de autenticação quanto à suscetibilidade ao ataque de SSID Confusion. A vulnerabilidade surge quando o SSID é empregado na geração da chave de criptografia durante o processo de autenticação. Um indicativo na cor laranja na tabela sinaliza que o protocolo de autenticação em questão está sujeito a vulnerabilidades sob determinadas circunstâncias.

WiFi Network Type	Authentication Type	Vulnerable
Home	WEP	✓
Home	WPA1	X
Home	WPA2	X
Home	WPA3	✓
Enterprise	802.11X / EAP	✓
Mesh	AMPE	✓
Other	FT	X
Other	FILS	✓

Figura 1 – Categoria de redes Wi_Fi.

Para redes domésticas, o protocolo WPA3, apesar de ser mais avançado que seus antecessores WPA1 e WPA2, apresenta uma vulnerabilidade específica ao ataque de SSID Confusion. Isso se deve a um modo opcional do WPA3 que não utiliza o SSID para criar a chave mestra emparelhada (PMK) durante o handshake SAE, tornando-o suscetível ao ataque mencionado. No contexto de redes corporativas, a vulnerabilidade é constante, já que a autenticação é realizada por meio do 802.1X e variações do EAP, que não dependem do SSID para a derivação do PMK. Quanto às redes mesh, elas seguem o mesmo padrão de vulnerabilidade das redes domésticas WPA3 sob as mesmas condições, devido ao uso do SAE. Redes mesh que empregam 802.1X também estão expostas ao ataque descrito.

O diagrama abaixo ilustra as fases do ataque de SSID Confusion.

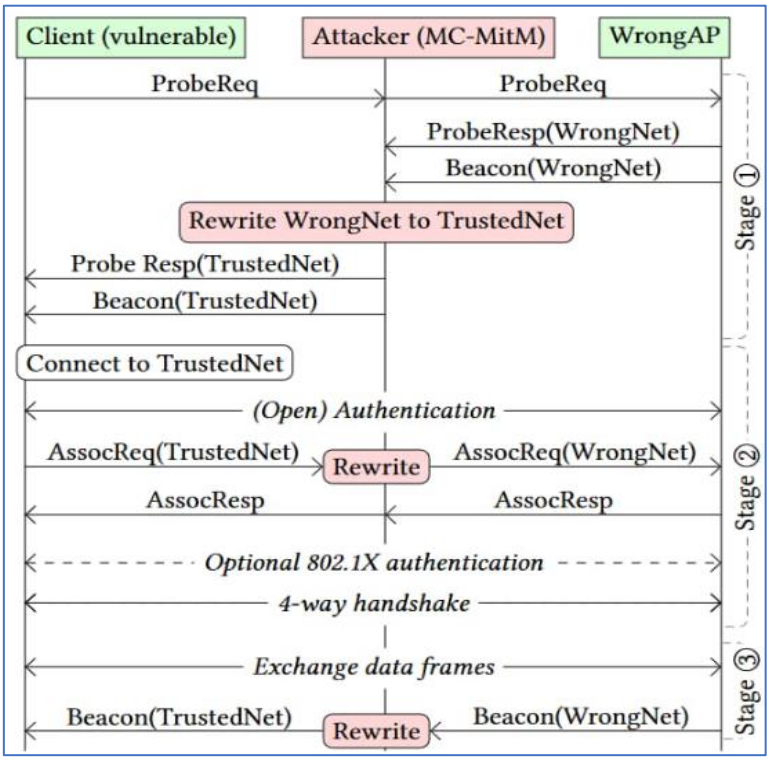


Figura 2 – Detalhes do ataque de SSID Confusion.

O ataque de SSID Confusion é uma técnica maliciosa que induz as vítimas a se conectarem a uma rede WiFi nociva. Ele explora vulnerabilidades na validação do SSID pelos dispositivos durante a configuração da conexão. Etapas do ataque consistem em, descoberta de rede, sequestro de autenticação, Man-in-the-Middle (MitM) Ativo. O atacante estabelece um ponto de acesso falso, denominado “WrongAP”, para promover a rede alvo falsa “WrongNet”. O MitM captura e altera pacotes WiFi para fazer o dispositivo da vítima detectar a “WrongNet” como uma rede segura. O invasor intercepta e modifica a autenticação do dispositivo para a “WrongNet”. O ataque MitM continua alterando dados em trânsito para manter a ilusão de que o dispositivo está conectado à rede segura e por fim um ataque bem-sucedido pode desativar conexões VPN ao enganar o dispositivo para reconhecer a “WrongNet” como uma rede segura, permitindo a inspeção e manipulação do tráfego pelo atacante.

3 RECOMENDAÇÕES

As recomendações para se defender contra ataques de SSID Confusion são:

Melhorias no padrão WiFi

- Atualizar o padrão WiFi 802.11 para exigir a autenticação do SSID ao conectar-se a uma rede protegida. Sempre inclua o SSID na derivação da chave durante o handshake de 4 vias ao conectar-se a redes protegidas, de maneira semelhante à forma como o protocolo Fast Transition (FT) lida com isso. Inclua o SSID como dados autenticados adicionais no handshake de 4 vias, permitindo que os clientes verifiquem com segurança o nome da rede.

Melhorias no cliente WiFi

- Melhorias na proteção de beacon ajudariam na defesa contra os ataques de confusão de SSID.

Evite a reutilização de credenciais

- As redes podem mitigar o ataque evitando a reutilização de credenciais entre SSIDs. As redes corporativas devem usar CommonNames de servidores RADIUS distintos, enquanto as redes domésticas devem usar uma senha exclusiva por SSID.

Uso adequado de VPN

- O uso habitual de uma VPN durante a conexão ao WiFi atenuará bastante as consequências desse ataque, pois o túnel criptografado impedirá que o adversário intercepte o tráfego mesmo após a execução bem-sucedida do ataque.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Top10Vpn
- Thehackernews

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH