BOLETIM DE SEGURANÇA

Nova falha crítica identificada na transferência do MOVEit, já sendo explorada em ataques.

heimdall
security research
A DIVISION OF ISH

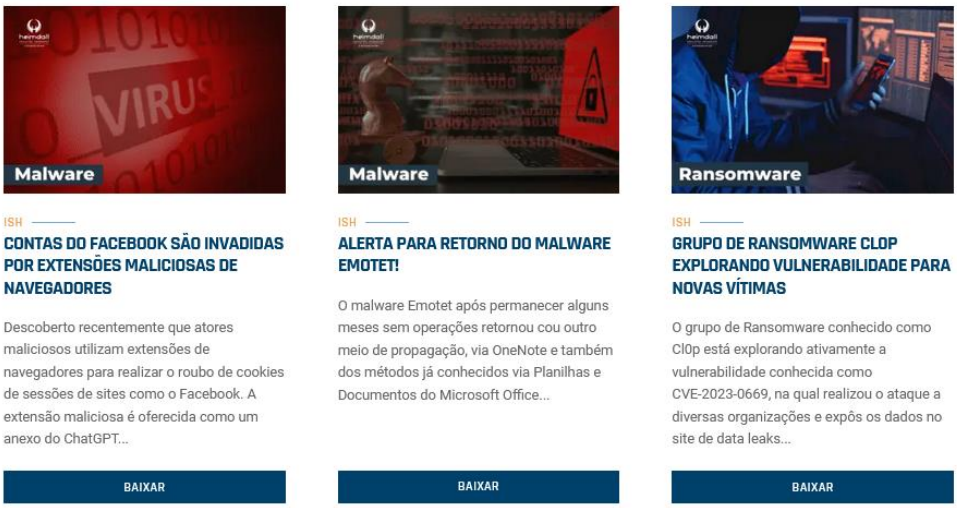
TLP: CLEAR

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente mantedores do MOVEit alertaram e lançaram patch de correção para a vulnerabilidade **CVE-2024-5806** de classificação crítica que diz respeito a um desvio de autenticação no Progress MOVEit Transfer (módulo SFTP) levando ao bypass de autenticação. Esta falha já está enfrentando tentativas de exploração logo após os detalhes do bug terem sido divulgados publicamente. Também a Progress alertou sobre outra vulnerabilidade crítica de bypass de autenticação associada ao **SFTP** (CVE-2024-5805, pontuação CVSS: 9.1) que afeta o **MOVEit Gateway** na versão **2024.0.0**.

2 DETALHES SOBRE AS FALHAS E EXPLORAÇÕES OBSERVADAS

CVE-2024-5806

Vulnerabilidade de autenticação inadequada no Progress MOVEit Transfer (módulo SFTP) pode levar ao desvio de autenticação.

Versões afetadas

- De 2023.0.0 anterior a 2023.0.11
- De 2023.1.0 anterior a 2023.1.6

Recomendação

Aplicar os patches de segurança disponibilizados para as versões afetadas.

Versões corrigidas

- 2023.0.11
- 2023.1.6
- 2024.0.2

Outras medidas são:

- Bloquear o acesso RDP de entrada ao MOVEit Transfer
- Limite o acesso de saída apenas a servidores confiáveis

Instâncias MOVEit expostas

Conforme a Censys, a maioria das instâncias MOVEit expostas que observadas estão nos EUA, com exposições adicionais observadas no Reino Unido, Alemanha, Holanda e Canadá, entre outros países.

Figura 1 – Mapa global de exposições MOVEit-Censys.

Já conforme a Shadowserver em uma publicação na sua página no X-antigo Twitter, a mesma alerta que já observaram tentativas de explorações sobre a vulnerabilidade nas instâncias MOVEit que estão publicamente disponíveis na Internet.

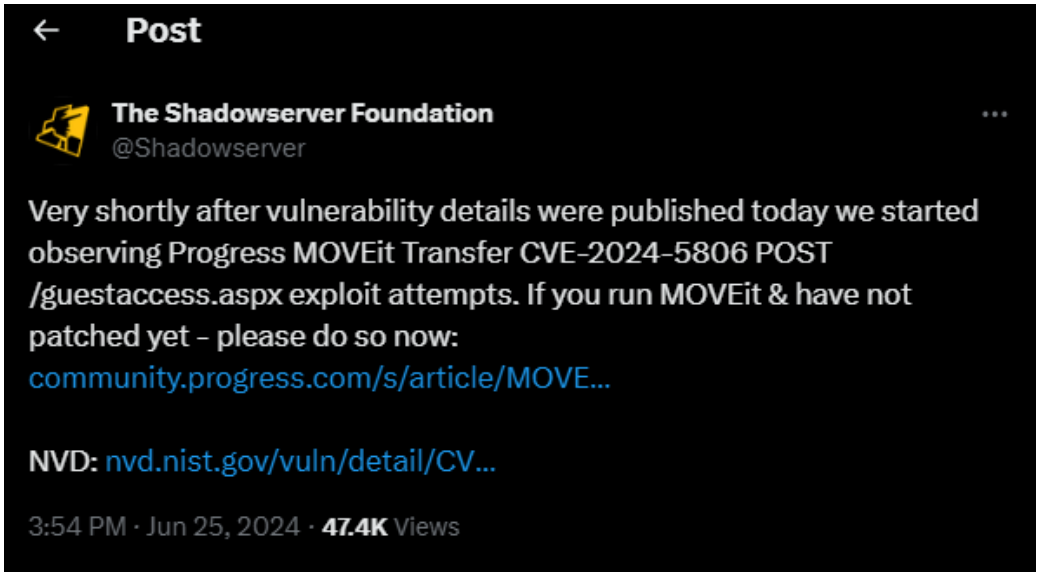


Figura 2 – Nota da Shadowserver no X.

CVE-2024-5805

Falha de desvio de autenticação no MOVEit gateway que permite o bypass de autenticação. O MOVEit gateway um serviço proxy projetado para facilitar implantações mais seguras do MOVEit Transfer.

Versão afetada

- MOVEit Gateway versão 2024.0.0

Recomendação

Aplicar o patch de segurança disponibilizado para a versão afetada.

Versão corrigida

- MOVEit Gateway 2024.0.1

3 CONCLUSÃO

Devido a explorações anteriores do MOVEit por atores maliciosos, as falhas de segurança citadas acima requerem uma notável atenção por partes dos administradores.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Progress MOVEit- CVE-2024-5806**
- **Progress MOVEit- CVE-2024-5805**
- **NVD**
- **Censys**
- **Shadowserver**
- **Thehackernews**

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH