Adobe corrige falha crítica do SessionReaper na plataforma de comércio e

Data: 2025-09-09 15:55:22

Autor: Inteligência Against Invaders

A Adobe está alertando sobre uma vulnerabilidade crítica (CVE-2025-54236) em suas plataformas

Commerce e Magento Open Source que os pesquisadores chamam de SessionReaper e descrevem

como uma das falhas “mais graves” da história do produto.

Hoje, a empresa de software lançou um patch para o problema de segurança que pode ser explorado sem autenticação para assumir o controle das contas dos clientes por meio doAPI REST do comércio.

De acordo com a empresa de segurança de comércio eletrônico Sansec, a Adobe notificou “clientes selecionados do Commerce” em 4 de setembro sobre uma correção de emergência planejada para 9 de setembro.

“A Adobe está planejando lançar uma atualização de segurança para Adobe Commerce e Magento Open Source na terça-feira, 9 de setembro de 2025”, diz o aviso.

“Esta atualização resolve uma vulnerabilidade crítica. A exploração bem-sucedida pode levar ao desvio do recurso de segurança.”

Os clientes que usam o Adobe Commerce on Cloud já estão protegidos por uma regra de firewall de aplicativo da Web (WAF) implantada pela Adobe como uma medida intermediária.

[IMAGEM REMOVIDA]Boletim de segurança de que não tem conhecimento de nenhuma atividade de exploração na natureza. Assessoria da Sansec também observa que os pesquisadores não viram nenhuma exploração ativa do SessionReaper.

No entanto, Sansec diz que um hotfix inicial para CVE-2025-54236 vazou na semana passada, o que pode dar aos agentes de ameaças uma vantagem potencial na criação de um exploit.

De acordo com os pesquisadores, a exploração bem-sucedida “parece” depender do armazenamento de dados da sessão no sistema de arquivos, uma configuração padrão que a maioria das lojas usa.

É altamente recomendável que os administradores testem e implantem o Patch disponível(download direto, arquivo ZIP) imediatamente. Os pesquisadores alertam que a correção desativa a funcionalidade interna do Magento que pode levar a alguma quebra de código personalizado ou externo.

Para o efeito, A Adobe atualizou sua documentação para alterações na injeção de parâmetro do construtor da API REST do Adobe Commerce.

“Por favor, aplique o hotfix o mais rápido possível. Se você não fizer isso, ficará vulnerável a esse problema de segurança e a Adobe terá meios limitados para ajudar a corrigir” – Adobe

Os pesquisadores da Sansec esperam que o CVE-2025-54236 seja abusado por meio da automação, em escala. Eles observam que a vulnerabilidade está entre as vulnerabilidades mais graves do Magento na história da plataforma, ao lado de Picada Cósmica, TrojanOrder, Ambionics SQLi e Roubar.

Problemas semelhantes no passado foram aproveitados para forjamento de sessão, escalonamento de privilégios, acesso a serviços internos e execução de código.

A empresa de segurança conseguiu reproduzir o exploit SessionReaper, mas não divulgou o código ou detalhes técnicos, dizendo apenas que “a vulnerabilidade segue um padrão familiar do ano passadoPicada Cósmicaataque.”

[IMAGEM REMOVIDA]