TLP: CLEAR

BOLETIM DE SEGURANÇA

Adobe emite correção para falha grave no ColdFusion

heimdall
security research

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

SUMÁRIO

LISTA DE TABELAS

1 INFORMAÇÕES SOBRE A VULNERABILIDADE

A Adobe lançou atualizações de segurança emergenciais para corrigir uma vulnerabilidade grave no **ColdFusion**, identificada como CVE-2024-53961. Essa falha, presente nas versões 2023 e 2021 do software, permite que invasores leiam arquivos arbitrários em servidores vulneráveis. A empresa destacou a gravidade do problema e a existência de um código de exploração de prova de conceito (PoC). Esta prova de conceito pode levar à leitura arbitrária do sistema de arquivos. A empresa alertou os clientes sobre a falha, classificando-a como "Prioridade 1" devido ao alto risco de ser explorada em versões específicas de produtos e plataformas.

A CVE-2024-53961 afeta as versões 2023.11, 2021.17 e anteriores do ColdFusion que possuem uma vulnerabilidade conhecida como 'Path Traversal', que permite a leitura arbitrária do sistema de arquivos. Essa falha pode ser explorada por invasores para acessar arquivos ou diretórios fora do diretório restrito do aplicativo, resultando na exposição de informações confidenciais ou na manipulação de dados do sistema.

Produto	Número	Plataforma
ColdFusion 2023	Atualização 11 e versões anteriores	Todas
ColdFusion 2021	Atualização 17 e versões anteriores	Todas

Tabela 1 – Versões afetadas.

Produto	Versão atualizada	Plataforma	Classificação de prioridade	Disponibilidade
ColdFusion 2023	Atualização 12	Todas	1	Nota técnica
ColdFusion 2021	Atualização 18	Todas	1	Nota técnica

Tabela 2 – Versões atualizadas.

2 RECOMENDAÇÕES

A Adobe recomenda que os administradores instalem urgentemente os patches de segurança lançados hoje (ColdFusion 2021 Update 18 e ColdFusion 2023 Update 12). Além disso, é importante seguir as configurações de segurança indicadas nos guias de bloqueio do ColdFusion 2023 e ColdFusion 2021.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Adobe**
- **NVD**
- **Bleepingcomputer**

4 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH