



# BOLETIM DE SEGURANÇA

Falha de Injeção SQL Crítica detectada no Fortra  
FileCatalyst Workflow



**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](#)



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	Sumário Executivo .....	4
2	Informação sobre a vulnerabilidade .....	5
3	Recomendações .....	6
4	Referências .....	7
5	Autor.....	8

## 1 SUMÁRIO EXECUTIVO

---

Foi descoberta a vulnerabilidade [CVE-2024-5276](#) categorizada como severidade crítica de segurança no Fortra FileCatalyst Workflow, permitindo que um atacante manipule o banco de dados do aplicativo.

## 2 INFORMAÇÃO SOBRE A VULNERABILIDADE

---

Identificada como [CVE-2024-5276](#), trata-se de uma vulnerabilidade de injeção de SQL no Fortra FileCatalyst Workflow que permite a um atacante alterar os dados do aplicativo. As consequências potenciais incluem a criação de usuários administrativos e a remoção ou alteração de dados no banco de dados do aplicativo. A extração de dados via injeção de SQL não é viável com esta vulnerabilidade. A exploração bem-sucedida não autenticada requer um sistema de fluxo de trabalho com acesso anônimo ativado; caso contrário, um usuário autenticado será necessário. Este problema está presente em todas as versões do FileCatalyst Workflow 5.1.6 Build 135 e anteriores.

A Fortra, afirmou que uma vulnerabilidade de injeção de SQL no Fortra FileCatalyst Workflow permite que um atacante altere os dados do aplicativo. Os impactos prováveis incluem a criação de usuários administrativos e a remoção ou alteração de dados no banco de dados do aplicativo. Foi enfatizado também que a exploração bem-sucedida não autenticada requer um sistema de fluxo de trabalho com acesso anônimo ativado. Alternativamente, também pode ser explorado por um usuário autenticado.

A empresa de segurança cibernética [Tenable](#), que relatou a falha em maio de 2024, lançou uma exploração de prova de conceito (PoC) para a falha. Um jobID fornecido pelo usuário é usado para formar a cláusula WHERE em uma consulta SQL. Um invasor remoto anônimo pode executar SQLi por meio do parâmetro JOBID em vários pontos de extremidade de URL do aplicativo Web de fluxo de trabalho.

### 3 RECOMENDAÇÕES

---

Atualizar para a versão 5.1.6 build 139 (ou posterior)

A Fortra recomenda para aqueles que não conseguem aplicar os patches imediatamente, podem desativar os servlets vulneráveis - csv\_servlet, pdf\_servlet, xml\_servlet e json\_servlet - no arquivo “web.xml” localizado no diretório de instalação do Apache Tomcat como soluções temporárias.

## 4 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Fortra](#)
- [Thehackernews](#)
- [NVD](#)

## 5 AUTOR

---

- Leonardo Oliveira Silva



heimdall  
security research

A DIVISION OF ISH