TLP: CLEAR

BOLETIM DE SEGURANÇA

Vulnerabilidades do FileCatalyst da Fortra foram corrigidas

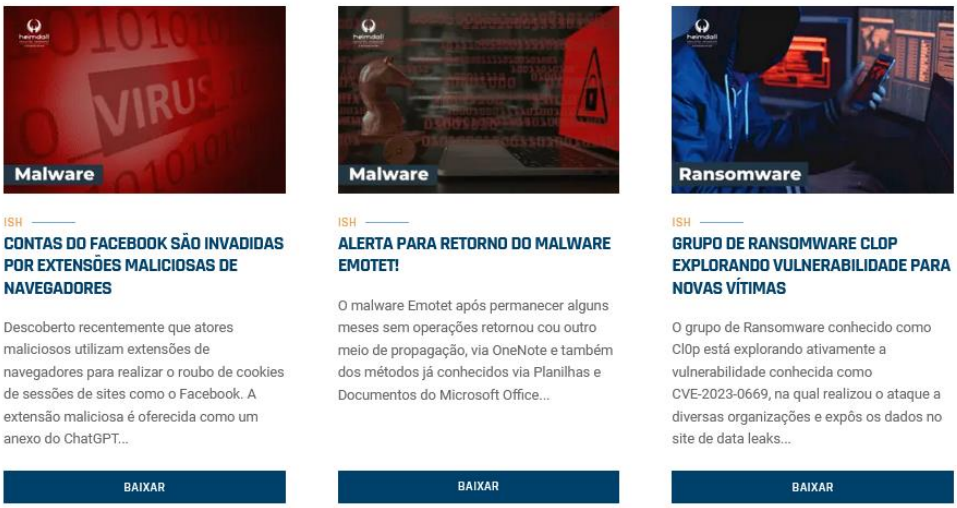
heimdall
security research
A DIVISION OF ISH

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 SOBRE AS VULNERABILIDADES NO FILECATALYST

A **Fortra** divulgou detalhes de uma falha crítica de segurança agora corrigida que afeta a solução de transferência de arquivos FileCatalyst, a qual poderia permitir que invasores não autenticados obtenham execução remota de código em servidores suscetíveis.

A vulnerabilidade foi identificada como **CVE-2024-25153**, apresentando uma base de pontuação de CVSS de **9,8 (crítica).**

De acordo com o comunicado da Fortra, "*um Directory Traversal dentro do "ftpservlet" do FIleCatalyst Workflow Web Portal permite que os arquivos sejam carregados para fora do diretório "uploadtemp" com uma solicitação POST especialmente criada*".

Também foi resolvido outras duas vulnerabilidades de segurança no FileCatalyst Direct, uma levando ao vazamento de informações e a outra execução de código remoto, sendo as CVEs:

- **CVE-2024-25154 –** Base de pontuação: 5,3 (médio)
- **CVE-2024-25155 –** Base de pontuação: 7.2 (alto)

As vulnerabilidades foram relatadas pela primeira vez em 09 de agosto de 2023 e corrigida dois dias depois no FileCatalyst Worflow na versão 5.1.6 Build 114 sem um identificador de CVE.

É valido salientar que o pesquisador de segurança Tom Wedgbury, da LRQA Nettitude, foi creditado por descobrir e relatar a falha e então, a empresa teria publicado a exploração completa da prova de conceito (PoC).

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CVE-2024-25153 – NVD**
- **CVE-2024-25154 – NVD**
- **CVE-2024-25155 – NVD**
- **Comunicado Fortra - CVEs**

heimdall
security research
A DIVISION OF ISH