Falhas críticas do servidor do Tableau permite uploads maliciosos de arquivos

Data: 2025-08-25 05:54:11

Autor: Inteligência Against Invaders

O Salesforce abordou várias vulnerabilidades críticas de segurança no Tableau Server e na área de trabalho que podem permitir que os invasores enviem arquivos maliciosos e executem código arbitrário.

As vulnerabilidades, divulgadas em 22 de agosto de 2025, foram identificadas proativamente durante uma avaliação de segurança e remendadas na liberação de manutenção de 22 de julho de 2025.

Vulnerabilidade de confusão do tipo crítico

A falha mais grave, CVE-2025-26496, obtém 9,6 críticos na escala CVSS e afeta os módulos de upload de arquivos em ambos [Servidor Tableau](#) e desktop.

Esse acesso de recurso usando vulnerabilidade incompatível de tipo permite a inclusão do código local, potencialmente permitindo que os invasores executem código malicioso no contexto do aplicativo. A falha afeta as instalações do Windows e do Linux em várias versões do produto.

Cve id	Tipo de vulnerabilidade	Pontuação CVSS V3	Nível de risco
CVE-2025-26496	Acesso de recurso usando tipo incompatível ('Tipo de confusão')	9.6	Crítico
CVE-2025-26497	Enviado irrestrito de arquivo com tipo perigoso	7.7	Alto
CVE-2025-26498	Enviado irrestrito de arquivo com tipo perigoso	7.7	Alto
CVE-2025-52450	Limitação inadequada de um nome de caminho para um diretório restrito ('Traversal do caminho')	8.5	Alto
CVE-2025-52451	Validação inadequada de entrada	8.5	Alto

Quatro vulnerabilidades adicionais centram -se nos recursos de upload de arquivo não restritos e fraquezas atravessadas.

O CVE-2025-26497 e o CVE-2025-26498 carregam pontuações CVSS de 7,7 e permitem a travessia

de caminho absoluto através de uploads perigosos de arquivos no editor de fluxo e estabelecer módulos de conexão-não-Undo, respectivamente.

Duas falhas de alta severidade, CVE-2025-52450AndCVE-2025-52451, afetam a funcionalidade Create-Data-Source-Source-Fil-File-File-File-File-File-File.

Ambas as vulnerabilidades pontuam 8,5 no CVSS e permitem [Traversal do caminho](#). Através de falhas inadequadas de limitação do nome do caminho e validação de entrada.

As vulnerabilidades impactam versões do servidor antes de 2025.1.4, 2024.2.13 e 2023.3.20. A falha de confusão do tipo também afeta as versões de desktop do Tableau correspondentes.

Todos os sistemas afetados são executados em plataformas Windows e Linux, com as vulnerabilidades direcionadas aos módulos específicos responsáveis ??pelo manuseio de arquivos e criação de fonte de dados.

Essas vulnerabilidades criam vários vetores de ataque para atores maliciosos. A combinação de uploads de arquivos irrestritos com recursos de travessia de caminho pode permitir que os atacantes reboquem arquivos para arbitrar os locais do sistema de arquivos do servidor.

A falha de confusão do tipo crítico aumenta a ameaça, possibilitando a execução do código, transformando vulnerabilidades de upload de arquivos em oportunidades completas de comprometimento do sistema.

Os módulos afetados lidam com a funcionalidade principal do Tableau, incluindo criação de origem de dados, edição de fluxo e estabelecimento de conexão, tornando essas vulnerabilidades particularmente perigosas para organizações que dependem do Tableau para operações de inteligência de negócios.

[Salesforce](#) aconselha fortemente todos os clientes do Tableau Server a atualizar imediatamente a versão mais recente suportada.

As correções foram incluídas nos lançamentos de manutenção publicados em 22 de julho de 2025, fornecendo uma janela de um mês entre a disponibilidade do patch e a divulgação pública.

As organizações devem priorizar os sistemas de patches expostos a usuários ou redes não confiáveis. Dada a natureza do upload de arquivo dessas vulnerabilidades, os administradores também devem revisar os controles de acesso em torno da criação de fonte de dados e funcionalidade de upload de arquivos enquanto planeja agendas de atualização.

Encontre esta notícia interessante! Siga -nos [Google News](#) Assim, [LinkedIn](#) X Para obter atualizações instantâneas!