CISA alerta sobre vulnerabilidade Dassault RCE explorada ativamente - Ag

Data: 2025-09-12 17:16:28

Autor: Inteligência Against Invaders

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) está alertando sobre hackers que exploram uma falha crítica de execução remota de código no DELMIA Apriso, uma solução de gerenciamento de operações de fabricação (MOM) e execução (MES) da empresa francesa Dassault Systèmes.

A agência acrescentou que a vulnerabilidade, rastreada como CVE-2025-5086 e classificado com uma pontuação de gravidade crítica (CVSS v3: 9.0), para as Vulnerabilidades Exploradas Conhecidas (KEV).

O DELMIA Apriso é utilizado em processos de produção para digitalização e monitoramento. As empresas em todo o mundo confiam nele para programar a produção, para o gerenciamento da qualidade, alocar recursos, o gerenciamento de armazéns e para a integração entre equipamentos de produção e aplicativos de negócios.

É normalmente implantado nas divisões automotiva, aeroespacial, eletrônica, de alta tecnologia e de maquinário industrial, onde o controle de alta qualidade, rastreabilidade, conformidade e um alto nível de padronização de processos são críticos.

A falha é uma vulnerabilidade de desserialização de dados não confiáveis que pode levar à execução remota de código (RCE).

O fornecedor divulgou o problema em 2 de junho, observando que afeta todas as versões do DELMIA Apriso desde o lançamento 2020 até o lançamento 2025, sem compartilhar muitos detalhes.

Em 3 de setembro, pesquisador de ameaças Johannes Ullrich publicou uma postagem no SANS ISC divulgando a observação de tentativas de exploração ativa aproveitando o CVE-2025-5086.

A exploração observada envolve o envio de uma solicitação SOAP maliciosa para endpoints vulneráveis que carrega e executa um executável .NET codificado em Base64 e compactado com GZIP incorporado no XML.

A carga útil real é um executável do Windows marcado como malicioso por Análise híbrida e sinalizado apenas por um motor em VírusTotal.

As solicitações maliciosas foram observadas com origem no IP 156.244.33[.]162, provavelmente associado a varreduras automatizadas.

A CISA não vinculou ao relatório Ullrich, então não está claro se este é o relatório que os levou a

adicionar CVE-2025-5086 ao KEV, ou se eles tivessem uma fonte separada confirmando a exploração.

A agência governamental dos EUA agora está dando ao setor empresarial federal até 2 de outubro para aplicar as atualizações ou mitigações de segurança disponíveis ou parar de usar o DELMIA Apriso.

Embora a orientação do BOD 22-01 seja vinculativa apenas para agências federais, organizações privadas em todo o mundo também devem considerar o aviso da CISA e tomar as medidas apropriadas.

[IMAGEM REMOVIDA]