TLP: CLEAR

BOLETIM DE SEGURANÇA

CISA alerta sobre exploração de vulnerabilidade na Oracle e Mitel

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 FIGURAS

1 INTRODUÇÃO EXECUTIVA

A **CISA** recentemente incluiu três vulnerabilidades no seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV) que estão sendo ativamente exploradas. Essas falhas de segurança, relacionadas aos sistemas **Oracle WebLogic Server** e **Mitel MiCollab**, possibilitam que invasores realizem ações administrativas não autorizadas e obtenham acesso a informações sensíveis de usuários e redes.

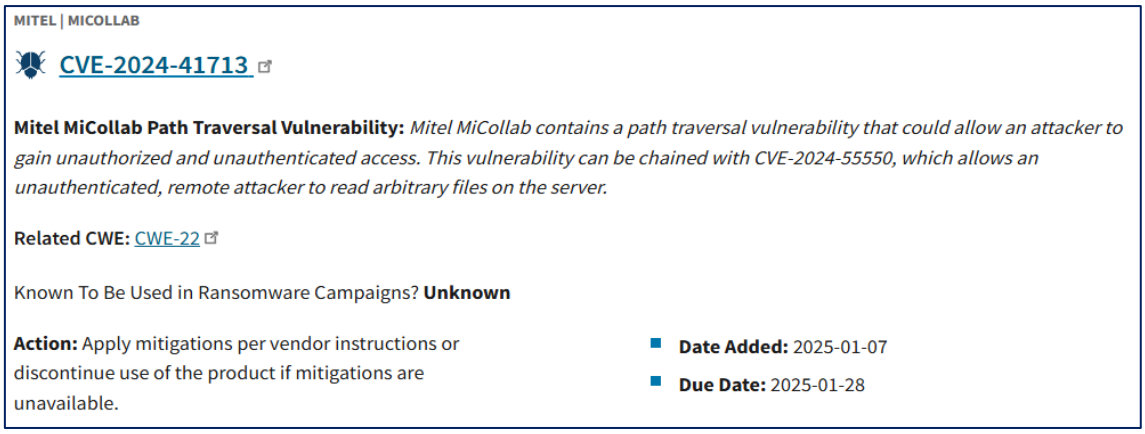

Figura 1 – Vulnerabilidade CVE-2024-41713 no Catálogo KEV-CISA.

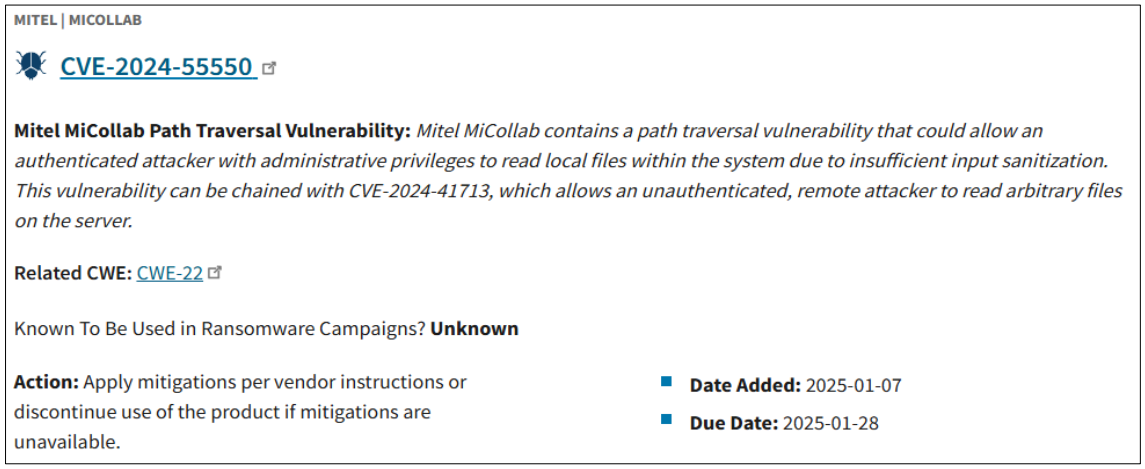

Figura 2 – Vulnerabilidade CVE-2024-55550 no Catálogo KEV-CISA.

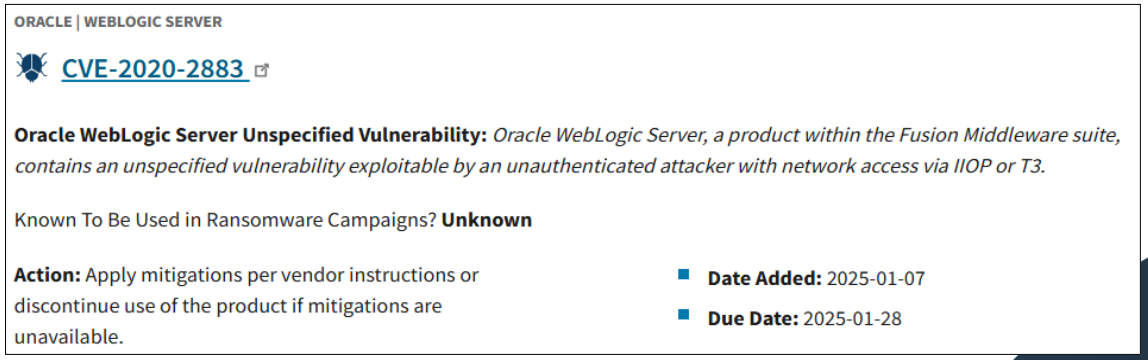

Figura 3 – Vulnerabilidade CVE-2024-2883 no Catálogo KEV-CISA.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Segue a lista de vulnerabilidades informadas pela CISA, juntamente com uma breve descrição de cada uma, incluindo o impacto potencial, componentes afetados.

CVE-2024-41713

Uma vulnerabilidade de *Path Traversal* identificada no componente **NuPoint Unified Messaging (NPM)** da plataforma de comunicações unificadas **MiCollab** da **Mitel**. Caso explorada, essa falha permite que invasores acessem informações de provisionamento sem autenticação, incluindo dados não confidenciais de usuários e redes, além de realizar ações administrativas não autorizadas no MiCollab Server. Esse problema pode ser combinado com a vulnerabilidade **CVE-2024-55550**, que possibilita a leitura de arquivos arbitrários no servidor por invasores remotos e não autenticados.

CVE-2024-55550

Outra vulnerabilidade de incluindo o impacto potencial, componentes afetados na solução **Mitel MiCollab**. Essa falha permite que invasores autenticados com privilégios administrativos leiam arquivos arbitrários em servidores afetados. Contudo, seu impacto é mais limitado, já que não viabiliza escalonamento de privilégios e os arquivos acessados não contêm informações sensíveis do sistema.

CVE-2020-2883

Identificada no **Oracle WebLogic Server** e corrigida há quatro anos, essa falha ainda é relevante, pois possibilita que invasores não autenticados, com acesso à rede via IIOP ou T3, comprometam o Oracle WebLogic Server. Um ataque bem-sucedido pode resultar no controle total do servidor, o que representa um grave risco de segurança.

3 RECOMENDAÇÕES

Embora o catálogo KEV se concentre em alertar as agências federais dos EUA sobre vulnerabilidades que devem ser corrigidas rapidamente, todas as organizações são recomendadas a priorizar a mitigação dessas falhas, mantendo seus sistemas atualizados e aplicando correções de segurança regularmente para reduzir os riscos de ataques em andamento e evitar a exploração ativa dessas brechas.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CISA**
- **CVE**
- **Bleeping Computer**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH