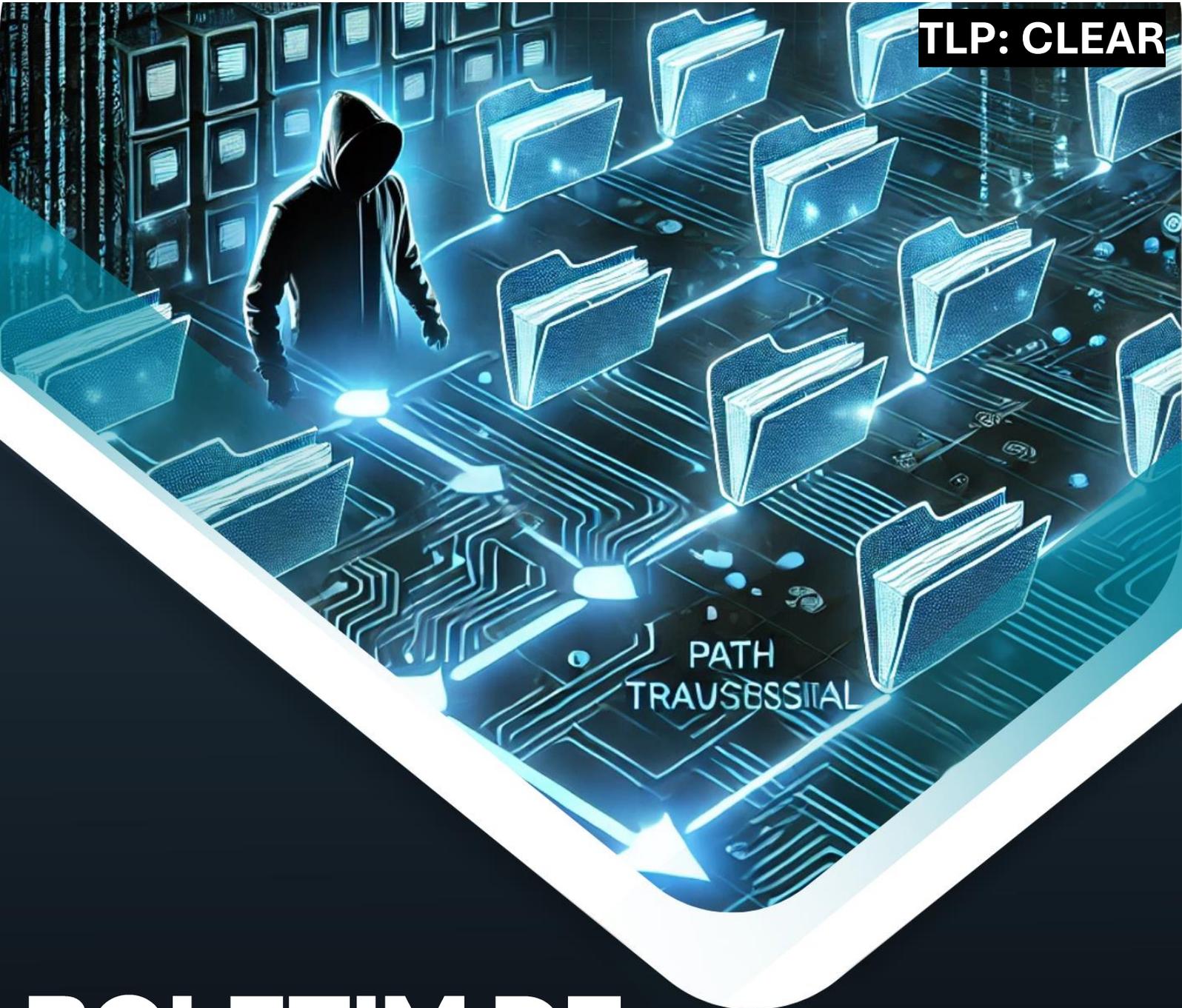


TLP: CLEAR



BOLETIM DE SEGURANÇA

**CISA alerta sobre exploração de vulnerabilidade na
Oracle e Mitel**

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



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	Introdução executiva.....	5
2	Informações sobre as vulnerabilidades.....	6
3	Recomendações.....	7
4	Referências	8
5	Autores.....	8

LISTA DE FIGURAS

Figura 1 – Vulnerabilidade CVE-2024-41713 no Catálogo KEV-CISA.	5
Figura 2 – Vulnerabilidade CVE-2024-55550 no Catálogo KEV-CISA.	5
Figura 3 – Vulnerabilidade CVE-2024-2883 no Catálogo KEV-CISA.	5

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.

MITEL | MICOLLAB

 [CVE-2024-41713](#) 

Mitel MiCollab Path Traversal Vulnerability: *Mitel MiCollab contains a path traversal vulnerability that could allow an attacker to gain unauthorized and unauthenticated access. This vulnerability can be chained with CVE-2024-55550, which allows an unauthenticated, remote attacker to read arbitrary files on the server.*

Related CWE: [CWE-22](#) 

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. ■ **Date Added:** 2025-01-07
■ **Due Date:** 2025-01-28

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

MITEL | MICOLLAB

 [CVE-2024-55550](#) 

Mitel MiCollab Path Traversal Vulnerability: *Mitel MiCollab contains a path traversal vulnerability that could allow an authenticated attacker with administrative privileges to read local files within the system due to insufficient input sanitization. This vulnerability can be chained with CVE-2024-41713, which allows an unauthenticated, remote attacker to read arbitrary files on the server.*

Related CWE: [CWE-22](#) 

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. ■ **Date Added:** 2025-01-07
■ **Due Date:** 2025-01-28

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

ORACLE | WEBLOGIC SERVER

 [CVE-2020-2883](#) 

Oracle WebLogic Server Unspecified Vulnerability: *Oracle WebLogic Server, a product within the Fusion Middleware suite, contains an unspecified vulnerability exploitable by an unauthenticated attacker with network access via ILOP or T3.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. ■ **Date Added:** 2025-01-07
■ **Due Date:** 2025-01-28

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 ILOP 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