TLP: CLEAR

BOLETIM DE SEGURANÇA

PoC para vulnerabilidade grave no Oracle WebLogic Server é divulgada

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

1 SUMÁRIO EXECUTIVO

Especialistas alertam sobre a divulgação pública de uma **Prova de Conceito (PoC)** para uma vulnerabilidade de gravidade alta que afeta o **Oracle WebLogic Server**. Identificada como CVE-2024-21182, essa falha representa um risco alto para organizações que utilizam o servidor, permitindo que invasores não autenticados com acesso à rede comprometam os sistemas alvo.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

Conforme a pesquisa, a **CVE-2024-21182** é considerada "facilmente explorável". Isso significa que atacantes não precisam de credenciais ou conhecimentos técnicos avançados para explorá-la, o que pode levar ao controle total do servidor comprometido. A vulnerabilidade pode ser explorada por meio dos protocolos **T3** e **IIOP** (**Internet Inter-ORB Protocol**), que geralmente estão ativados por padrão para comunicações remotas. As versões impactadas incluem *12.2.1.4.0* e *14.1.1.0.0* do **Oracle WebLogic Server**, amplamente empregadas no ambiente corporativo para implantação de aplicativos empresariais.

As preocupações relacionadas à essa vulnerabilidade cresceram significativamente após a publicação de um **exploit** no GitHub por um usuário identificado como "**k4it0k1d**". O repositório disponibiliza uma Prova de Conceito (PoC) funcional, o que facilita o acesso de possíveis atacantes. Além disso, atualizações compartilhadas em redes sociais, como a plataforma X (antiga Twitter), contribuíram para ampliar a visibilidade dessa vulnerabilidade.

3 RECOMENDAÇÕES

Dado o impacto potencial dessa vulnerabilidade, organizações que utilizam o Oracle WebLogic Server devem agir imediatamente para mitigar os riscos. As seguintes medidas são recomendadas:

- **Aplicação do patch oficial:** A Oracle deve lançar um patch de segurança em sua próxima Critical Patch Update (CPU). Enquanto isso, as organizações devem consultar as orientações da Oracle para aplicar mitigações temporárias.
- **Desabilitar T3 e IIOP:** Se esses protocolos não forem essenciais, desativá-los pode reduzir significativamente a superfície de ataque.
- **Monitoramento de tráfego de rede:** Ferramentas de monitoramento devem ser usadas para identificar atividades suspeitas ou tentativas de acesso não autorizado.
- **Restringir acesso à rede:** Utilizar firewalls ou VPNs para limitar o acesso às instâncias do WebLogic Server.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NVD**
- **GitHub**
- **GBHackers**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH