TLP: CLEAR


# BOLETIM DE SEGURANÇA

## Oracle publica Critical Patch Updates de janeiro de 2025 com correções de vulnerabilidades em seus principais produtos

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 INTRODUÇÃO EXECUTIVA

Recentemente, a Oracle lançou uma a **atualização crítica de Patches** abordando **318 vulnerabilidades** em diversos produtos. Dentre essas, destacam-se várias falhas críticas que podem permitir a invasores comprometerem sistemas afetados. Este relatório detalha as principais CVEs mencionadas, fornecendo informações técnicas, sistemas afetados, impactos e recomendações para mitigação.

## 2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Entre essas falhas, a mais crítica afeta o *Oracle Agile Product Lifecycle Management (PLM) Framework*, catalogada como **CVE-2025-21556**, com uma pontuação **CVSS de 9,9**. Essa vulnerabilidade pode permitir que agentes mal-intencionados assumam o controle total de sistemas vulneráveis. Além disso, a Oracle também corrigiu outras vulnerabilidades críticas com uma pontuação **CVSS de 9,8**, destacando-se as seguintes:

**CVE-2025-21524**

- Vulnerabilidade no componente Monitoring and Diagnostics SEC do JD Edwards EnterpriseOne Tools. Permite que atacantes não autenticados com acesso via rede comprometam o componente afetado, potencialmente resultando em execução remota de código.

**CVE-2023-3961**

- Vulnerabilidade no componente E1 Dev Platform Tech (Samba) do JD Edwards EnterpriseOne Tools. A exploração pode permitir que atacantes executem código arbitrário no sistema afetado, comprometendo sua integridade e disponibilidade.

**CVE-2024-23807**

- Vulnerabilidade no componente Apache Xerces C++ XML parser do Oracle Agile Engineering Data Management. Falha que pode ser explorada para causar negação de serviço ou execução de código arbitrário através de documentos XML malformados.

**CVE-2023-46604**

- Vulnerabilidade no componente Apache ActiveMQ do Oracle Communications Diameter Signaling Router. Permite que atacantes enviem mensagens maliciosas que podem resultar em execução remota de código ou interrupção do serviço.

**CVE-2024-45492**

- Vulnerabilidade no componente XML parser (libexpat) presente em vários produtos Oracle, incluindo Communications Network Analytics Data Director e Financial Services Behavior Detection Platform. A exploração pode levar à execução de código arbitrário ou negação de serviço através de entradas XML especialmente criadas.

**CVE-2025-21535**

- Vulnerabilidade no componente Core do Oracle WebLogic Server. Permite que atacantes não autenticados com acesso via IIOP ou T3 comprometam o servidor, resultando em execução remota de código.

**CVE-2016-1000027**

- Vulnerabilidade no componente Spring Framework do Oracle BI Publisher. Falha que pode ser explorada para execução remota de código devido a deserialização insegura de dados.

  **CVE-2023-29824**

- Vulnerabilidade no componente Analytics Server (SciPy) do Oracle Business Intelligence Enterprise Edition. Permite que atacantes executem código arbitrário no servidor de análises através de vetores não especificados.

Para mais detalhes, visite a página de alertas da Oracle referente à Atualização Crítica de Patches de janeiro de 2025.

## 2.1 SISTEMAS E PRODUTOS AFETADOS

As vulnerabilidades mencionadas afetam uma ampla gama de produtos Oracle, incluindo:

- Oracle Agile Product Lifecycle Management Framework versão *9.3.6*
- JD Edwards EnterpriseOne Tools (Monitoring and Diagnostics SEC) versão *9.2.5.5* e anteriores
- JD Edwards EnterpriseOne Tools (E1 Dev Platform Tech - Samba) versão *9.2.5.4* e anteriores
- Oracle Agile Engineering Data Management versão: *9.3.5* e anteriores
- Oracle Communications Diameter Signaling Router versão *8.4.0* e anteriores
- Oracle Fusion Middleware versão *12.2.1.4.0* e *14.1.1.0.0*

## 2.2 IMPACTO DA VULNERABILIDADE

A exploração dessas vulnerabilidades pode resultar em:

- Comprometimento total do sistema afetado.
- Acesso não autorizado a informações sensíveis.
- Possível interrupção das operações de negócios.
- Elevação de privilégios, permitindo ações maliciosas adicionais.
- Execução remota de código sem necessidade de autenticação.

# 3 RECOMENDAÇÕES

Para minimizar os riscos associados às vulnerabilidades críticas recentemente divulgadas nos produtos da Oracle, é essencial que as organizações adotem as seguintes medidas de segurança:

**Aplicação imediata dos patches de segurança**

- Recomenda-se a aplicação imediata dos patches fornecidos no Critical Patch Update - January 2025, garantindo que todos os sistemas estejam protegidos contra possíveis explorações.

**Monitoramento contínuo e análise de logs**

- Implemente um sistema de monitoramento contínuo para detectar comportamentos suspeitos e atividades anômalas nos ambientes afetados. A análise detalhada dos logs pode ajudar a identificar tentativas de exploração das falhas corrigidas.

**Atualização de ferramentas de segurança**

- Mantenha atualizados os sistemas de segurança, como firewalls, IDS/IPS (Intrusion Detection/Prevention Systems) e soluções antivírus, garantindo que possam detectar e bloquear atividades maliciosas associadas às vulnerabilidades mencionadas.

**Restrição de acesso remoto**

- Para minimizar a exposição dos sistemas, restrinja acessos remotos, utilize VPNs seguras e implemente autenticação multifator (MFA) para proteger credenciais e evitar acessos não autorizados.

# 4 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Oracle**
- **NVD**
- **The Hacker News**


# 5 AUTORES


- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH