NCSC emite alerta sobre exploração ativa da vulnerabilidade de dia 0 do O

Data: 2025-10-07 07:21:31

Autor: Inteligência Against Invaders

O Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) emitiu um alerta de segurança

após a confirmação da exploração ativa de uma vulnerabilidade crítica de dia 0, rastreada como

CVE-2025-61882, no Oracle E-Business Suite (EBS).

A Oracle lançou um comunicado urgenteatualização de segurançapara resolver o problema, ressaltando o risco imediato para as organizações que executam versões afetadas do EBS.

Falha crítica de execução remota de código no Oracle EBS

CVE-2025-61882 é uma vulnerabilidade grave de execução remota de código identificada no componente BI Publisher Integration do Oracle Concurrent Processing no EBS.

De acordo com o comunicado da Oracle, a falha permite que um invasor remoto e não autenticado envie solicitações HTTP especialmente criadas para uma instância vulnerável do EBS, resultando no comprometimento total do sistema subjacente sem exigir interação do usuário.

Atributo	Valor
ID do CVE	CVE-2025-61882
Produto	Oracle E-Business Suite
Componente	Integração do BI Publisher (Oracle Concurrent Processing)
Tipo de vulnerabilidade	Execução Remota de Código
Pontuação CVSS 3.1	9.8 (crítico)
Vetor de ataque	Rede

A vulnerabilidade afeta as versões 12.2.3 a 12.2.14 do Oracle EBS, representando o maior risco para organizações que expuseram suas implantações do Oracle EBS à Internet pública.

Com uma pontuação básica do CVSS v3.1 de 9,8, a Oracle confirmou o vulnerabilidade está sendo explorado ativamente, permitindo que os agentes de ameaças obtenham acesso não autorizado e executem comandos arbitrários.

A Oracle listou vários indicadores de comprometimento (IoCs), incluindo endereços IP suspeitos (200.107.207.26 e 185.181.60.11), comandos conhecidos para conexões de saída e hashes SHA256 de arquivos de exploração relacionados, para ajudar as organizações na detecção e resposta.

Etapas de orientação e mitigação

O NCSC insta todas as organizações que executam versões afetadas do Oracle EBS a avaliarem imediatamente se há comprometimento de seus ambientes. As principais recomendações incluem:

- Realize uma avaliação de comprometimento usando os IoCs publicados na consultoria da Oracle.
- **Relate incidentes suspeitos:** As organizações afetadas no Reino Unido devem entrar em contato com o Oracle PSIRT e notificar o NCSC por meio do portal de relatórios.
- **Aplique atualizações de segurança:** Instale a atualização mais recente do Oracle EBS, garantindo que a atualização crítica do patch de outubro de 2023 esteja em vigor com antecedência.
- **Reforce a exposição da rede**: limite o acesso direto à Internet ao Oracle EBS e siga as diretrizes de implantação da Oracle. O NCSC também fornece práticas recomendadas para proteger perímetros de rede.
- **Monitoramento contínuo:** Mantenha monitoramento de rede robusto e caça a ameaças para detectar e conter atividades maliciosas.

O NCSC reitera a importância de reduzir a superfície de ataque, minimizando o software acessível externamente.

Para organizações onde a exposição à Internet é necessária, os controles de segurança e a segmentação são essenciais.