Oracle lançou patch para o pacote de negócios E (CVE-2025-61882) após c

Data: 2025-10-06 18:07:01

Autor: Inteligência Against Invaders

boletim de segurança da informação

há 6 horas
Alerta, Vulnerabilidades

A Oracle emitiu uma atualização de emergência para ***consertar*** um sério problema de segurança em seu E-Business Suite, que foi alvo de recentes ataques de roubo de dados Cl0p.

O ***crítico*** vulnerabilidade, CVE-2025-61882 (pontuação CVSS: 9,8), pode permitir que um invasor não autenticado com acesso HTTP comprometa o componente Oracle Concurrent Processing.

“Essa vulnerabilidade é explorável remotamente sem autenticação, ou seja, pode ser explorada em uma rede sem a necessidade de um nome de usuário e senha”, disse a Oracle em um comunicado. “Se explorada com sucesso, essa vulnerabilidade pode resultar na execução remota de código.”

Em um alerta separado, o diretor de segurança da Oracle, Rob Duhart ***dito*** a empresa lançou correções para CVE-2025-61882 para “fornecer atualizações contra exploração potencial adicional que foram descobertas durante nossa investigação”.

A vulnerabilidade de dia zero no Oracle foi relatada, após notícias de ransomware Cl0p direcionado ao Oracle E-Business Suite. A Mandiant, de propriedade do Google, chamou isso de “campanha de e-mail de alto volume” usando muitas contas hackeadas.

Em uma postagem compartilhada no LinkedIn, Charles Carmakal, CTO da Mandiant no Google Cloud, disse “ O Cl0p explorou várias vulnerabilidades no Oracle EBS, o que lhes permitiu roubar grandes quantidades de dados de várias vítimas em agosto de 2025?, acrescentando que “várias vulnerabilidades foram exploradas, incluindo vulnerabilidades que foram corrigidas na atualização de julho de 2025 da Oracle, bem como uma que foi corrigida neste fim de semana (CVE-2025-61882)”.

“Dada a ampla exploração em massa de dia zero que já ocorreu (e a exploração de n dias que provavelmente continuará por outros atores), independentemente de quando o patch for aplicado, as organizações devem examinar se já foram comprometidas”, observou Carmakal.