O Oracle confirma que os hackers segmentam dados do E-Business Suite

Data: 2025-10-03 10:12:37

Autor: Inteligência Against Invaders

A Oracle confirmou que um grupo de hackers roubou dados de seus aplicativos do E-Business Suite

(EBS) e está usando as informações em campanhas de extorsão.

A empresa alerta que esses invasores exploram vulnerabilidades já corrigidas na Atualização de patches críticos (CPU) de julho de 2025.

A Oracle pede fortemente a todos os clientes que apliquem a CPU mais recente imediatamente para se defender contra outras invasões.

Os executivos e as equipes de TI em várias grandes organizações receberam e -mails de extorsão alegando que seus dados do Oracle EBS foram copiados.

Os hackers exigem resgates de até US $ 50 milhões para impedir a liberação do público. A empresa de segurança cibernética Halcyon, que está respondendo a incidentes, diz que o grupo se identifica como ligado ao CL0P Ransomware Gang.

As vítimas receberam capturas de tela, listas de arquivos e provas de registros roubados para fazer backup das ameaças.

Detalhes da campanha

Os atacantes começaram a enviar ameaças por e-mail antes de 29 de setembro, usando centenas de contas comprometidas de terceiros.

As notas apresentavam inglês pobre e gramática, uma marca registrada das comunicações CL0P. Pelo menos uma empresa reconheceu publicamente que seus dados do EBS foram exfiltrados.

De acordo com Genevieve Stark, do Google Threat Intelligence Group, um dos endereços usados ??nas notas de extorsão estava anteriormente vinculado a um afiliado do CL0P.

Cynthia Kaiser, de Halcyon, explica que o CL0P é conhecido pela massa furtiva roubo de dados e altas demandas de resgate. Em incidentes anteriores de alto perfil, o grupo explorou falhas no software Moveit File-Transfer para roubar dados de centenas de organizações.

O CL0P tem como alvo grandes empresas como Shell, British Airways e BBC, exigindo grandes pagamentos para evitar vazamentos de dados.

Os invasores teriam abusado de funções padrão de retenção de senha em portais EBs voltados para a Internet. No entanto, alguns especialistas acreditam que a violação decorreu de uma

vulnerabilidade do EBS abordada na CPU de julho.

Oracle's investigação está em andamento, e a empresa ainda não comentou o método exato de intrusão.

Todos os clientes da Oracle EBS devem verificar se a CPU de julho de 2025 foi aplicada a todas as instâncias. As organizações ainda usando níveis mais antigos de patches enfrentam maior risco de roubo e extorsão de dados.

As equipes de segurança devem revisar os logs de acesso para obter atividades suspeitas de retenção de senha e monitorar contas de terceiros para sinais de compromisso.

Além disso, os clientes devem implementar uma forte autenticação de vários fatores para acesso ao EBS e restringir as funções administrativas a redes confiáveis.

Verifique regularmente a integridade do sistema com varreduras automatizadas e mantenha backups offline para garantir uma rápida recuperação.

A Oracle continua colaborando com os parceiros policiais e de segurança cibernética para rastrear a campanha e apoiar os clientes afetados.

A aplicação da CPU de julho de 2025 continua sendo a primeira etapa crítica em proteger os ambientes de suíte de e-business em relação a essas ameaças de extorsão.