CrowdStrike vincula Oracle EBS RCE (CVE-2025-61882) a ataques Cl0p ini

Data: 2025-10-07 09:04:41

Autor: Inteligência Against Invaders

CrowdStrike vincula Oracle EBS RCE (CVE-2025-61882) a ataques Cl0p iniciados em 9 de agosto de 2025

A CrowdStrike vincula a falha CVE-2025-61882 (CVSS 9.8) do Oracle EBS ao Cl0p, permitindo o RCE não autenticado, explorado pela primeira vez em 9 de agosto de 2025.

Os pesquisadores da CrowdStrike atribuíram com confiança moderada a exploração de Falha do Oracle E-Business Suite CVE-2025-61882 (CVSS 9.8) para o Grupo Cl0p, também conhecido como Graceful Spider. O bug crítico permite a execução remota de código não autenticado, com os primeiros ataques conhecidos rastreados até 9 de agosto de 2025.

*“A CrowdStrike Intelligence avalia com confiança moderada que*ARANHA GRACIOSA*provavelmente está envolvido nesta campanha, mas não pode descartar a possibilidade de que vários agentes de ameaças tenham explorado o CVE-2025-61882.” lê o* relatório *publicado pela CrowdStrike. “A primeira exploração conhecida ocorreu em 9 de agosto de 2025; no entanto, as investigações continuam em andamento e esta data está sujeita a alterações.*

Esta semana, a Oracle lançou um patch de emergência para resolver essa falha crítica em seu E-Business Suite.

*“Atualizado [10/04/2025]: A Oracle emitiu*Alerta de segurança da OracleAdvisory– CVE-2025-61882 *para fornecer atualizações contra exploração potencial adicional que foram descobertos durante nossa investigação.” diz o*alerta*publicado pela empresa.”Recomendamos fortemente que os clientes do Oracle E-Business Suite (EBS) apliquem as orientações fornecidas por este Alerta de Segurança o mais rápido possível.”*

A falha foi explorada peloCl0p ransomwaregrupo em ataques de roubo de dados. Invasores remotos não autenticados podem explorar a falha para assumir o controle do componente Oracle Concurrent Processing.

O CVE-2025-61882 afeta o Oracle E-Business Suite 12.2.3–12.2.14 (BI Publisher Integration), especialistas alertam que é facilmente explorável via HTTP.

*“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.” lê o*Consultivo*. “A Oracle recomenda enfaticamente que os clientes apliquem as atualizações fornecidas por este Alerta de Segurança o mais rápido possível.”*

A CrowdStrike adverte que a divulgação de um POC em 3 de outubro e o patch CVE-2025-61882 da Oracle quase certamente estimularão os agentes de ameaças, especialmente aqueles familiarizados com o Oracle EBS, a desenvolver POCs armados e direcionar instâncias do EBS expostas à Internet.

Em 29 de setembro de 2025, o grupo Cl0p enviou um e-mail para organizações alegando roubo de dados do Oracle EBS. Em 3 de outubro, um canal do Telegram vinculado a Aranha Dispersa, Aranha escorregadia (Lapsus$) e Caçadores brilhantes postou um suposto exploit do Oracle EBS e criticou o grupo Cl0p. A origem e a reutilização não são claras, no entanto, a Oracle publicou o POC como um IOC e se alinha com a exploração baseada em servlet observada.

"Enquanto a análise está em andamento, o suposto POC parece estar alinhado com pelo menos parte da exploração observada, incluindo alavancagem de atividadesJava Servletspara exploração." continua Crowdstrike.

A atividade observada da Crowdstrike começando com um HTTP POST para **/OA_HTML/SyncServlet** para ignorar a autenticação (às vezes abusando de uma conta de administrador do EBS). Os invasores então visam o Oracle **Gerenciador de modelos do editor XML**Usando **/OA_HTML/RF.jsp** e **/OA_HTML/OA.jsp** para carregar um modelo XSLT malicioso cuja visualização executa comandos. Nomes de predefinições em **xdo_templates_vl** corresponder às referências de URL.
A execução bem-sucedida abre uma conexão TLS de saída (porta 443) com a infraestrutura do invasor, usada para carregar shells da Web para execução e persistência de comandos.

Em alguns casos, os invasores usam dois arquivos: **FileUtils.java**, que faz o download do segundo arquivo e **Log4jConfigQpgsubFilter.java**, que atua como backdoor. Juntos, eles instalam um shell da Web que é acionado quando alguém visita uma URL de ajuda pública (/OA_HTML/help/...). O shell da Web executa o código diretamente na memória, permitindo que o invasor execute comandos sem gravar arquivos no disco.

"A CrowdStrike Intelligence avalia que um ou mais agentes de ameaças quase certamente aproveitaram uma nova vulnerabilidade de dia zero (agora rastreada como CVE-2025-61882) noA campanha de exploração em massa discutida neste artigo. Essa avaliação é feita com alta confiança com base na exploração observada, uma revisão inicial do POC carregado e o aviso de segurança da Oracle de 4 de outubro de 2025." conclui a Crowdstrike.

Equipe HUNTER da Resecurity**Lançado**Uma análise separada e abrangente de cargas maliciosas plantadas por agentes de ameaças no resultado da exploração. Os ataques do CL0P exploram uma cadeia do lado do servidor, usando injeção de SSRF e CRLF para forçar os servidores EBS a buscar e executar cargas XSL maliciosas, alcançando a execução remota de código (RCE) sem artefatos baseados em disco. Os invasores também aproveitam as caixas de correio comprometidas para abusar dos fluxos de redefinição de senha da conta local do EBS, ignorando as proteções SSO/MFA para roubar credenciais e exfiltrar dados confidenciais.

Esta semana, a CISA dos EUA também Adicionado a vulnerabilidade CVE-2025-61882 ao seu catálogo de vulnerabilidades exploradas conhecidas. A CISA ordena que as agências federais corrijam a falha até 27 de outubro de 2025.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Oracle)