O Google CodeMender está aqui! Quando a IA encontra bugs no código e

Data: 2025-10-07 14:04:56

Autor: Inteligência Against Invaders

Redazione RHC**:7 Outubro 2025 15:27**

Seria fantástico **ter um agente de IA capaz de analisar automaticamente o código de nossos projetos, identificar bugs de segurança, gerar correções e liberá-los imediatamente em produção.** No entanto, parece que teremos que nos acostumar com essa ideia: a inteligência artificial promete que tudo isso não é mais ficção científica, mas uma realidade que se aproxima.

Google DeepMind revelou **CodeMender** um **Novo agente de inteligência artificial** projetado para *Encontre e corrija vulnerabilidades automaticamente no código do software.* De acordo com o Blog oficial da empresa , o sistema combina *os recursos dos grandes modelos de linguagem do Gemini Deep Think com um conjunto de ferramentas para análise e validação de patches,* permitindo que as correções de bugs sejam feitas com mais rapidez e precisão do que os métodos tradicionais.

Os desenvolvedores apontam que, mesmo usando ferramentas como OSS-Fuzz e Grande sono , **Corrigir vulnerabilidades manualmente continua sendo um processo trabalhoso.** O CodeMender aborda esse problema de forma abrangente: *Ele não apenas responde a novos problemas criando patches automaticamente, mas também reescreve proativamente fragmentos de código, eliminando classes inteiras de vulnerabilidades.*

Nos últimos seis meses, a equipe da DeepMind contribuiu **72 patches de segurança para projetos de código aberto.** Esses incluem *bibliotecas totalizando mais de 4,5 milhões de linhas de código.* Todas as alterações *são revisados quanto à correção e estilo antes de serem submetidos à revisão humana.*

O CodeMender aproveita os modelos Gemini para analisar a lógica do programa, analisar o comportamento do código e verificar automaticamente os resultados. O agente também pode *Verifique se o patch aborda a causa raiz da vulnerabilidade e não causa regressões.*

Para tornar o processo confiável, a DeepMind implementou novos métodos de análise: **análise estática e dinâmica, teste diferencial, fuzzing e solucionadores SMT.** Além disso, o CodeMender é baseado em um sistema multiagente, com módulos individuais especializados em diferentes aspectos da revisão de código, desde a comparação de alterações até a autocorreção.

Em um exemplo, **CodeMender** *corrigido um estouro de buffer no analisador XML identificando um erro no gerenciamento da pilha de elementos, em vez do local real da falha.* Em outro caso, o agente **propôs uma correção complexa relacionada ao ciclo de vida do objeto e à geração de código C dentro do projeto.**

O CodeMender também é capaz de **reescrever o código existente usando estruturas de dados e APIs mais seguras.** Por exemplo, o agente adicionou automaticamente *-fbounds-segurança* anotações ao Libwebp biblioteca para *Evite estouros de buffer.* Esta biblioteca foi afetada anteriormente pela vulnerabilidade crítica CVE-2023-4863, usado no Exploração do iPhone do NSO Group . Os pesquisadores estimam que, com as novas anotações, esses ataques não serão mais possíveis.

O agente não apenas aplica patches, mas também os testa automaticamente, corrigindo novos erros e verificando sua conformidade funcional com o código-fonte. Se forem detectadas inconsistências, o sistema usa um “juiz LLM” para corrigir o patch sem intervenção humana.

Por enquanto *A DeepMind está mantendo uma postura cautelosa: todas as alterações estão sujeitas à revisão manual obrigatória.* No entanto, o CodeMender já está ajudando a melhorar a segurança de dezenas de projetos populares de código aberto. **A empresa pretende expandir seu envolvimento com a comunidade e disponibilizar a ferramenta para todos os desenvolvedores no futuro.**

Os desenvolvedores prometem publicar relatórios técnicos e artigos sobre as abordagens usadas no CodeMender nos próximos meses. Eles dizem que o projeto está apenas começando a explorar o potencial da inteligência artificial na segurança de software.

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