**Programiści na celowniku. Krytyczna luka w Cursor IDE**

**Cursor IDE, jedno z najpopularniejszych narzędzi programistycznych wspieranych przez sztuczną inteligencją, był podatny na ataki hakerskie. To efekt luki, która pozwalała na zdalne wykonanie dowolnego kodu bez wiedzy użytkownika. Sytuacja umożliwiała uzyskanie stałego dostępu do komputera dewelopera oraz modyfikowanie projektów nad którymi pracowano – ostrzegają eksperci firmy Check Point Research.**

- *Narzędzia programistyczne oparte na sztucznej inteligencji zmieniają sposób tworzenia oprogramowania, ale jednocześnie tworzą nowe wektory ataków oparte na zaufaniu. MCPoison pokazuje, jak łatwo można wykorzystać automatyzację i wygodę do cichej, długotrwałej eksploatacji w środowiskach współdzielonego kodowania* – powiedział Oded Vanunu, szef działu badań nad podatnościami w produktach w firmie Check Point Software.

Autorzy badania zapewniają, że atak wykorzystujący lukę systemową CVE-2025-54136 (nazwaną MCPoison) nie jest czysto teoretyczny. W środowiskach zespołowych (gdzie projekty są współdzielone przez repozytoria) wystarczyło, żeby jedna osoba miała dostęp do zapisu, by zainfekować MCP i rozprzestrzenić zagrożenie. Mechanizm przypomina cybernetycznego konia trojańskiego, z tą różnicą, że użytkownik sam otwiera drzwi.

*- Atak mógł być całkowicie niewidoczny i powtarzany przy każdym uruchomieniu projektu –* zaznaczają eksperci Check Point Research. Wszystko sprowadza się do tzw. MCP (*Model Context Protocol*) czyli plików konfiguracyjnych w Cursorze, które określają, jak AI ma działać w konkretnym projekcie. W normalnych warunkach użytkownik akceptuje MCP raz, przy pierwszym uruchomieniu. Problem w tym, że nikt już nie sprawdza, czy zawartość tego pliku się zmieniła.

Badacze bezpieczeństwa cybernetycznego odkryli, że po jednorazowej akceptacji pliku MCP, można go później dowolnie zmodyfikować, np. wstawiając złośliwy kod, który otwiera tylne drzwi (ang. *backdoor*), wysyła dane do zewnętrznego serwera lub uruchamia skrypty. Co najgorsze – za każdym razem, gdy ofiara otwiera projekt, kod uruchamia się automatycznie i bez ostrzeżeń.

Dla firm i zespołów deweloperskich oznacza to realne ryzyko:

l **Ciągły, niewidoczny dostęp** do środowiska ofiary przez osoby postronne,

l **Ekspozycję haseł, tokenów API, kluczy chmurowych** i innych wrażliwych danych,

l **Zagrożenie dla kodu źródłowego**, własności intelektualnej oraz danych klientów,

l **Utratę zaufania do automatyzacji AI**, która miała zwiększać bezpieczeństwo i efektywność.

Check Point poinformował twórców Cursor IDE o luce 16 lipca 2025 roku. Naprawa została udostępniona dwa tygodnie później, 30 lipca. To jednak nie koniec problemu – ekspertom zależy, by cała branża zaczęła inaczej podchodzić do zaufania w narzędziach opartych na AI.

**Co powinni zrobić menedżerowie IT i zespoły programistyczne?**

**Przede wszystkim należy traktować pliki MCP jak kod źródłowy**, przeglądać je, kontrolować wersje i ograniczyć do nich dostęp. **Nie wolno ślepo ufać automatyzacji AI**, nawet jeśli coś wygląda na nieszkodliwe, warto wiedzieć, co robi. Analitycy Check Pointa zalecają również **ograniczanie uprawnień w repozytoriach**, ponieważ dostęp do zapisu powinien być przemyślany.

Odkrycie podatności CVE-2025-54136 (in. MCPoison) pokazuje, że nawet narzędzia tworzone z myślą o zwiększeniu produktywności mogą stać się wektorem ataku. W dobie rosnącej integracji AI w środowiskach programistycznych – od IDE po CI/CD – kluczowe jest, by bezpieczeństwo szło w parze z innowacją.

**Szczegóły wraz z wideo-wizualizacją ataku dostępne są pod** [**tym linkiem**](https://research.checkpoint.com/2025/cursor-vulnerability-mcpoison/)**.**