

Forenzički izveštaj [FR821UK734]

Nadležni forenzičar: John Doe

Uzorak podnesen od strane: JiSecBlue

Adresa entiteta koji je podneo uzorak: Bulevar oslobođenja 17, Novi Sad

Naziv pretnje: NpmHydra

Opis ponašanja: Zlonamerni paket kompromituje CI/CD procese i ubacuje skriveni kod.

Nivo pretnje: Nizak

Heš uzorka: f6a9e7d3574f1c1b21826ca091513f85

Sažetak

NpmHydra je malver usmeren na npm ekosistem koji kompromituje pakete kroz lanac zavisnosti. Nakon infekcije, krade tokene i omogućava daljinski pristup napadaču. Preporučuje se hitna rotacija kredencijala i detaljna analiza svih zahvaćenih repozitorijuma.