

Forenzički izveštaj [FR456UK358]

Nadležni forenzičar: John Doe

Uzorak podnesen od strane: JiSecBlue

Adresa entiteta koji je podneo uzorak: Knez Mihailova 1, Beograd

Naziv pretnje: NpmHydra

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

Nivo pretnje: Visok

Heš uzorka: a8ca8b357568669e99d7f68cc2151ae5

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.