

Forenzički izveštaj [FR576UK195]

Nadležni forenzičar: John Doe

Uzorak podnesen od strane: JiSecBlue

Adresa entiteta koji je podneo uzorak: Trg slobode 1, Novi Sad

Naziv pretnje: NodePhantom

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

Nivo pretnje: Kritičan

Heš uzorka: 068c6cc3f09d60fe612bda6d690a51a6

Sažetak

NodePhantom 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.