Microsoft Teams

Vulnerabilitet në Microsoft Teams që mund të çojë në marrjen e llogarive

Platforma e bashkëpunimit e Microsoft Teams përmban një dobësi që mund të shfrytëzohet me një GIF me qëllim të keq i cili i mundëson një sulmuesi të marrë llogaritë e Teams të një kompanie.

Problemi qëndron në dy sub-domain të Teams që ishin të prekshëm nga vulnerabiliteti, aadsync-test.teams.microsoft.com dhe data-dev.teams.microsoft.com. Pasi zoteron domainin,sulmuesi mund ta përdore atë për të marrë një çertifikatë të dixhitale te vlefshme gjë që i lejon atij të ketë akses në bazën e te dhenave te llogarisë së Teams, të shkruaj të dhëna ose të vjedhi llogarinë.

Mashtrimi që një sulmues përdor është një GIF me qëllim të keq, në ndryshim me një link të thjeshtë, të cilën shumë njerëz tani e dinë që nuk duhet ta klikojnë. Procesi fillon duke dërguar një imazh tek një viktimë me një atribut "src" të vendosur në sub-domainin e kompromentuar përmes bisedave të Ekipeve. Kur objektivi hap këtë mesazh, shfletuesi i viktimës do të përpiqet të ngarkojë imazhin dhe kjo do ta dërgojë cookie-un authtoken në sub-domainin e kompromentuar domethënë direkt në duart e sulmuesit.Kjo i siguron sulmuesit mundesinë për të fshire të gjitha të dhënat e viktimës.

Mbas zbulimit Microsoft Teams ka nxierre një update të rëndësishem per te ndrequr këtë vulnerabilitet ,kështu që azhurnoni menjëherë aplikacionin e Teams.