DNSC: Vulnerabilitate critica de securitate cibernetica, descoperita la nivelul Cisco

O vulnerabilitate critica de securitate cibernetica, prin care un atacator neautentificat poate avea acces la retea, folosind date de autentificare generate identic în anumite versiuni si platforme, a fost identificata la nivelul Cisco, informeaza Directoratul National de Securitatea Cibernetica (DNSC), într-un comunicat de presa publicat vineri.

"CVE-2025-20286 este o vulnerabilitate critica cu scor CVSS de 9.9, ce afecteaza instantele Cisco Identity Services Engine (ISE) implementate în Amazon Web Services (AWS), Azure si Oracle Cloud Infrastructure (OCI). Aceasta permite unui atacator neautentificat, cu acces la retea, sa compromita alte instante ISE din cloud folosind date de autentificare generate identic în anumite versiuni si platforme. Problema apare deoarece, în timpul implementarii ISE în cloud, sunt generate aceleasi date de autentificare pentru toate instantele care ruleaza aceeasi versiune pe aceeasi platforma cloud. Aceste date nu difera între instante, ceea ce permite reutilizarea lor pentru a obtine acces la alte implementari similare", mentioneaza expertii DNSC.

Potrivit sursei citate, exploatarea cu succes a acestei vulnerabilitati poate permite unui atacator sa acceseze informatiile sensibile stocate în instantele Cisco ISE din AWS, sa modifice configuratiile critice ale sistemului, sa perturbe functionarea normala a serviciilor de autentificare si autorizare si compromiterea întregii infrastructuri de securitate a retelei, permitând accesul neautorizat la resursele organizatiei.

"Vulnerabilitatea afecteaza instantele ISE doar daca nodul de administrare principal (Primary Administration Node) este implementat în infrastructura de tip cloud. Daca acesta este instalat în infrastructura fizica locala a organizatiei, sistemul nu este afectat", noteaza Directoratul.

Lista de recomandari din partea specialistilor în securitate cibernetica include: aplicarea patch-urilor oficiale furnizate de Cisco pentru versiunile afectate din mediile cloud (AWS, Azure, OCI); restrictionarea accesului la nivel de IP prin configurarea Security Groups si filtrare în interfata Cisco ISE; segmentarea retelei pentru a izola instantele ISE de alte resurse sensibile ale infrastructurii; executarea resetarii configuratiei (application reset-config ise) în cazul instalarilor noi în cloud, pentru regenerarea datelor de acces; evitarea restaurarii backup-urilor realizate înainte de aplicarea remediilor, deoarece pot reinjecta vulnerabilitatea.