

# BULETINI JAVOR

## 8-12 JANAR 2024



Shprehja

"Siguria kibernetike nuk ka të bëjë vetëm me mbrojtjen e të dhënave; ka të bëjë me mbrojtjen e së ardhmes së inovacionit, integritetin e sistemeve tona dhe besimi i një bote digjitale."

e javës

Përmbajtja:

- Fjala e Zv.Kryeministres në konferencën vjetore lidhur me progresin e arritur në fushën e sigurisë kibernetike
- CISA paralajmëron për shfrytëzim aktiv të një vulnerabiliteti të Microsoft SharePoint
- GitLab - patching alert



### Fjala e Zv.Kryeministres në konferencën vjetore lidhur me progresin e arritur në fushën e sigurisë kibernetike

Në konferencën për shtyp lidhur me prioritetet në Infrastrukturë, Zv.Kryeministrja Belinda Balluku në fjalën e saj theksoi progresin e arritur në fushën e sigurisë kibernetike duke përfshirë reformën legislative si dhe ngritjen e Qendrës Operacionale të Monitorimit.

Gjithashtu në përbushje të objektivave për të arritur standartet ndërkombëtare në fushën e sigurisë kibernetike, u theksua edhe ngritja e laboratoreve si pjesë e rëndësishme e SOC Kombëtar



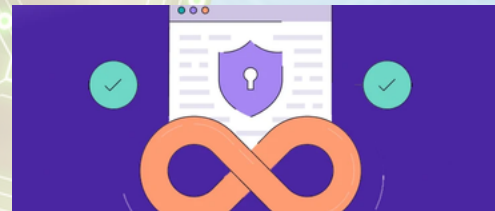
### CISA paralajmëron për shfrytëzim aktiv të një vulnerabiliteti të Microsoft SharePoint

Agjencia Amerikane për Sigurinë Kibernetike dhe Sigurinë e Infrastrukturës (CISA) ka shtuar një vulnerabilitet kritik të sigurisë, në katalogun e saj të Vulnerabiliteteve të Shfrytëzuara (KEV), i cili ndikon në serverin Microsoft SharePoint.

Vulnerabiliteti i identifikuar si CVE-2023-29357 ( CVSS: 9.8), është një e metë e përshtatshme të privilegjit që mund të shfrytëzohet nga një sulmues për të fituar privilegje administratori.

[Link: Lexo më shumë](#)

### PATCHING ALERT



### GitLab - patching alert

GitLab ka publikuar së fundmi përditësime sigurie për të adresuar dy vulnerabilitete kritike. Një nga vulnerabilitetet kritike është si rezultat i një gabimi në procesin e verifikimit të emailit, i cili lejon përdoruesit të rivendosin fjalëkalimin e tyre përmes një adrese emaili dytësor.

Për të zbutur çdo kërcënim të mundshëm, këshillohet që të përmirësoni instancat në një version të *patchuar* sa më shpejt të jetë e mundur dhe të aktivizoni 2FA, veçanërisht për përdoruesit me privilegje të larta.

[Link:Lexo më shumë](#)