

CVE-2026-30388: User Enumeration via Timing Attack in iRODS Native Authentication

John Constable
john@metadata.school



Timing gap exposes valid usernames



~224ms ($\sigma \approx 34$ ms)

~246ms ($\sigma \approx 32$ ms)



$\Delta \approx 22$ ms (9.6%) — enough to fingerprint valid usernames remotely

Full write-up, PoC & methodology → github.com/metadata-school/irods_vulnerability_explorations

Found with A.I. assistance in February - the models will only get better.
Bulk of the time was verifying the findings, making the write-up useful.