21, April 2025
Reported By :: Zhaenx
Contact :: zhaenx.101@gmail.com

Title	***A01:2021 – Broken Access Control (OWASP Top 10)***
URL-Endpoint	***1. https://portal.gcore.com/accounts/profile/users***
Evidence	***BrokenAccessControl_PoC.mp4***
Severity	***Critical***

DESCRIPTION

The ***"Invite User"*** feature in the Gcore service contains a logic vulnerability that allows an attacker to abuse the authentication flow by:

1. Locking the victim's email so that they cannot sign up for the Gcore service,
2. And after the victim successfully logs in, the attacker can still force the user to log out of the application by removing their email from the invite list.

This vulnerability allows for control over the access status of another person's email, without any interaction from the victim. It also creates an opportunity for large-scale attacks, such as preventing new user onboarding or disrupting the user experience en masse.

STEP TO REPRODUCE

1. The attacker logs in to his Gcore account (for example, aureleaugliest@ptct.net).
2. The attacker uses the ***"Invite User"*** feature to invite the victim's unregistered email (for example, joyannconvincing@ptct.net).
3. The system sends a verification email to the victim's email, but the victim ignores the email (because he doesn't know the sender).
4. The victim tries to register a Gcore account normally, but an error message appears: *"Client with email anetta8@ptct.net already exists."*
5. The victim then uses the ***"Forgot Password"*** feature, successfully changes the password, and logs in.
6. [Optional Step]➔ The attacker can:
   - Remove the victim from the user list (resulting in a forced logout), or
   - Not remove them, which leaves the victim permanently under the attacker's organization.

IMPACT

1. **Global Email Lockout:** Attackers can "lock" anyone's email so they can't sign up.
2. **Access Control to Logged-in Users:** Even after a victim successfully signs up, an attacker can still force the user out of the system (force logout).
3. **Potential for Large-Scale Abuse:** Attackers can invite multiple emails to prevent potential users/clients from signing up.
4. **Bypass Verification Process**: Users can sign in without accepting the invitation, but are still treated as part of the attacker's team.
5. **Authentication Integrity Violation**: There is no clear separation of access rights between ***"invited users"*** and ***"registered users"***.
6. **Attackers can restrict victim access:**
   - Victims cannot become admins for new accounts with their email.
   - The victim becomes a permanent part of the attacker's ***"user list"*** , unless the attacker deletes or releases the victim's email.

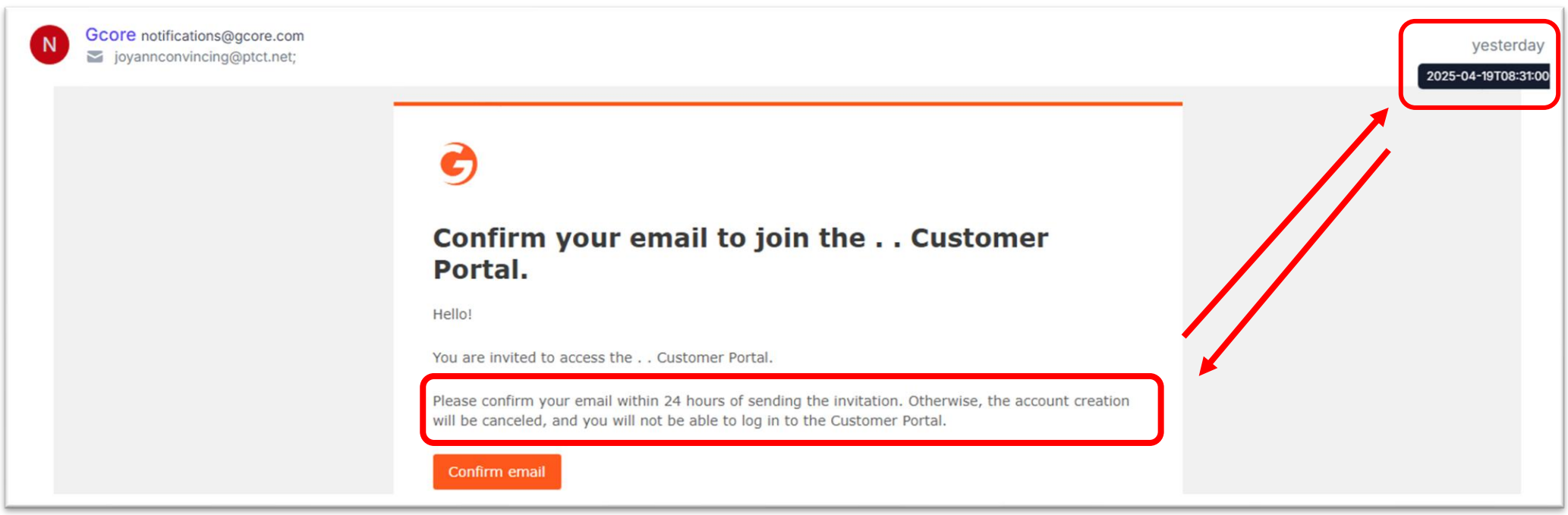
RECOMMENDATION

1. Separate ***"invite", "registered",*** and ***"confirmed"*** statuses explicitly.
2. Don't lock emails just because they've been invited — new emails shouldn't be considered users until they actually sign up.
3. Once the email is executed and the self-login is complete, the user must be disconnected from the inviting organization, unless they expressly agree to it.

Notes (Additional info):

1. The system treats emails that are simply "invited" as if they were already active accounts, and the system also fails to distinguish between "invited users" and "self-registered users", This indicates a logical misconfiguration in the system that could be exploited by a malicious user.
2. **Expired Invitation Not Working**

   The system states that the invitation link is ***only valid for 24 hours***, in fact:
   - After 24 hours had passed, the victim's email (joyannconvincing@ptct.net) still could not be registered.
   - This happens because the email is still listed on the attacker's dashboard as an active invitation.
   - This means that the system does not perform the ***automatic deletion function (auto-expire)*** as promised or written in the email.



Impact : The invitation does not expire even after 24 hours, so the victim remains permanently locked out.