Loomo / Nbo2o / Willand 子域名探查報告

測試時間：2026-07-11
測試者：Linux Hermes
範圍：25 個子域名（loomo 11 + nbo2o 1 + willand 13）
本機出口：43.160.194.36

關鍵發現總結

風險	發現
HIGH	`logsec.ninebot.com` 生產 log 服務公開 + Actuator/Prometheus 暴露 18 個 IoT API 端點
HIGH	`navimow-bond/prod/test/uat.willand.com` IoT Bond 後台 3 個實例公開
MEDIUM	`fleet-web-dev.willand.com` Fleet DEV 環境公開
MEDIUM	`navimow-app-h5-dev.willand.com` App DEV 環境公開
MEDIUM	`marketplace-api-dev/stress.navimow.com` Marketplace DEV/Stress API 公開（後端 502）
MEDIUM	`logsec-fra(-tmp).willand.com` 測試環境公開 + Spring Boot Actuator
LOW	`www.nbo2o.com` 重定向 bug — 跳到 `www.www.nbo2o.com`
LOW	loomo.com 4 個子域名 SSL 過期（loomo/www.loomo/mx/support）
INFO	將近一半 loomo 子域名 DNS 不存在（已退役）
INFO	2 個 dev-pay/ww7/www willand 子域名 DNS 不存在

W1. logsec.ninebot.com — 生產 IoT log 服務公開【HIGH】

漏洞描述

`logsec.ninebot.com` 是 Segway-Ninebot 的 IoT log 安全服務生產環境域名，直接在公網暴露。通過 Spring Boot Actuator 可以訪問 Prometheus metrics 端點。

Prometheus Metrics 洩漏的內部 API 表面

從 `/actuator/prometheus` 的 `interfaceName` 標籤提取出全部 18 個 IoT 內部 API 端點：

端點	功能（推測）
`/upload/v4/init`	Multipart upload init
`/upload/v4/uploadPart`	上傳分片
`/upload/v4/completeMultipartUpload`	完成上傳
`/upload/v4/abortMultipartUpload`	中止上傳
`/upload/v4/listMultipartUploads`	列出進行中上傳
`/upload/v4/abortTask`	中止任務
`/upload/v4/updateRemark`	更新備註
`/upload/v2/abortTask`	V2 任務中止
`/upload/v2/completeTask`	V2 任務完成
`/upload/v2/url`	V2 上傳 URL
`/upload/post`	上傳 POST
`/upload/url`	上傳 URL
`/upload/heartbeat`	心跳（公開可達返回 success）
`/vehicle/file/get`	取得車輛文件
`/vehicle/file/version/upload`	上傳車輛文件版本
`/task/abortTask`	任務中止
`/task/log/cmd`	任務 log 命令
`/test/hello`	測試端點（返回 "hello world"）

證據鏈

Actuator 公開：

```
curl https://logsec.ninebot.com/actuator
# → {"_links":{"self":{"href":"http://logsec.ninebot.com/actuator"},...,
#     "prometheus":{"href":"http://logsec.ninebot.com/actuator/prometheus"},
#     "health":{...},"health-path":{...}}}
```

Prometheus Metrics 真實可達（200, 691 行）：

```
application="iot-log-service-api",region="eu",
disk_total_bytes{path="/data/service/iot-log-service-api-eu/.",region="eu",} 2.74743689216E11
jvm_memory_used_bytes{area="heap",id="G1 Old Gen",region="eu",} 3.525448336E9
iot_log_service_interface_request_time_seconds_count{
  application="iot-log-service-api",
  interfaceName="/upload/v4/uploadPart",region="eu",
} 2.8977903E7
```

確認 API 活的：

```
curl https://logsec.ninebot.com/upload/heartbeat
# → {"resultCode":"1000","resultDesc":"success","data":null,"t":...}

curl https://logsec.ninebot.com/test/hello
# → hello world

curl https://logsec.ninebot.com/upload/v4/init?deviceId=test
# → {"resultCode":"1009","resultDesc":"param invalid","data":null,...}
#  ← 後端處理請求但要求 POST + JSON body
```

元數據洩漏

從 Prometheus 標籤洩漏：
- 應用名稱: `iot-log-service-api`
- 區域: `eu`（歐洲）
- 磁盤路徑: `/data/service/iot-log-service-api-eu/.`
- 磁盤大小: 274 GB
- JVM heap: 3.5 GB Old Gen
- 線程峰值: 257

修復建議

- 限制 `logsec.ninebot.com` 僅內網/VPN 訪問
- 移除 Prometheus 端點公網訪問（或加 IP 白名單）
- 從 `/test/hello` 等測試端點移除
- 從 Prometheus 標籤移除應用內部路徑/區域

W2. navimow-bond(.test/.uat).willand.com — IoT 配對後台 3 個實例公開【HIGH】

漏洞描述

`navimow-bond.willand.com`、`navimow-bond-test.willand.com`、`navimow-bond-uat.willand.com` 三個實例全部公開，是 Navimow 智能割草機的 IoT 配對/綁定後台。

證據鏈

頁面內容：

```
<title>Nivamow Bond</title>
<meta name="description" content="Nivamow Bond - Nivamow Amdin Dashbord" />
```

注意拼寫錯誤：
- "Nivamow" 應該是 "Navimow"（typo）
- "Amdin" 應該是 "Admin"（typo）
- "Dashbord" 應該是 "Dashboard"（typo）

3 個實例的 md5 不同（確認為不同部署）：
- prod: `a683d36c45aab1c15a6178a65a9abf13`
- test: `74466b85fafe0f5eb3c9f46d3b8e1ee4`
- uat: `db8865923fdc167f80e1795c6bfedb0e`

不同環境用不同 marketplace API：
- prod: `https://marketplace-fra-api.navimow.com`
- test: `https://marketplace-api-dev.navimow.com`
- uat: `https://marketplace-api-stress.navimow.com`

修復建議

- test/uat 環境應限制內網訪問
- 修正頁面拼寫錯誤（暴露內部代碼未審計）
- 統一 marketplace API endpoint

W3. fleet-web-dev.willand.com — Fleet DEV 環境公開【MEDIUM】

漏洞描述

NavimowFleet IoT 車隊管理後台的開發環境公開。

證據鏈

```
curl https://fleet-web-dev.willand.com/
# → <title>NavimowFleet</title>
# → 7924 bytes SPA
# → x-azure-ref: ... Azure Front Door
```

修復建議

- DEV 環境限制內網或加 IP 白名單
- 定期輪換認證

W4. navimow-app-h5-dev.willand.com — App DEV 環境公開【MEDIUM】

漏洞描述

Navimow App 的 H5 開發版本公開。

證據鏈

```
<title>Navimow</title>
<link rel="preconnect" href="https://navimow-h5-fra.willand.com">
```

- 大小：1993 bytes
- Vite/React 應用
- Azure Front Door 託管

修復建議

- DEV 環境限制內網或加 IP 白名單

W5. marketplace-api-{dev,stress}.navimow.com — Marketplace API 公開【MEDIUM】

漏洞描述

`marketplace-api-dev.navimow.com` 和 `marketplace-api-stress.navimow.com` 是 Navimow 應用商城的 DEV 和 Stress 環境 API。

證據

從 `navimow-bond-test` 和 `navimow-bond-uat` JS bundle 發現這兩個端點。

當前狀態：所有端點返回 502 Bad Gateway（Azure Application Gateway 後端掛了）。

但端點存在且公開，如果後端恢復就是可攻擊面。

修復建議

- DEV/Stress API 限制內網訪問
- 加 IP 白名單

W6. logsec-fra(-tmp).willand.com — 測試環境【MEDIUM】

漏洞描述

`logsec-fra.willand.com` 和 `logsec-fra-tmp.willand.com` 是 logsec 的測試環境，Actuator 公開。

證據鏈

```
curl https://logsec-fra.willand.com/actuator
# → {"_links":{"self":{"href":"http://logsec.ninebot.com/actuator"},...}}
# ↑ HATEOAS self 指向生產域名 logsec.ninebot.com（生產 hostname 洩漏）

curl https://logsec-fra.willand.com/health
# → {"status": "healthy", "service": "default-site"}
```

修復建議

- 測試環境限制內網
- 不要在 HATEOAS 暴露生產域名（使用環境變量）

W7. www.nbo2o.com 重定向 bug【LOW】

漏洞描述

`www.nbo2o.com` 重定向到 `www.www.nbo2o.com`（域名配置 bug，雙 "www"）。

證據

```
HTTP/1.1 301 Moved Permanently
Location: http://www.www.nbo2o.com/
Server: nginx
X-NWS-LOG-UUID: 14508852978872431310
```

修復建議

- 修正 Nginx 配置，去掉重複的 "www"

W8. loomo.com 多個 SSL 過期【LOW】

漏洞描述

loomo.com 主域及子域名 SSL 證書全部過期 ~10 個月。

受影響

- loomo.com
- www.loomo.com
- mx.loomo.com
- support.loomo.com

修復建議

- 立即續期 SSL 證書
- 或重新部署 loomo 服務（5 個子域名 DNS 已不存在 = 已退役？）

W9. loomo / willand 子域名 DNS 退役【INFO】

退役 / 不存在

loomo.com（5 個子域名）：
- blog, comingsoon, shop, shopping, store — 全部 DNS 不存在

willand.com（3 個）：
- dev-pay, ww7, www — DNS 不存在

意味著：許多舊服務已退役，但 DNS 記錄未清理（subdomain takeover 風險面）

W10. Navimow Bond「IoT 配對」業務流程【INFO】

從 JS bundle 提取的業務關鍵字：
- "Nivamow Bond"（typo）
- "Amdin Dashbord"（typo）
- `/bond/*` 系列端點
- Marketplace API 整合

Navimow 割草機的 IoT 配對流程：
1. 設備首次開機
2. 透過 Navimow APP 連接到 WiFi
3. APP 呼叫 bond 服務 配對
4. 配對後設備加入用戶帳號
5. 透過 marketplace 服務下載功能/地圖

最終累計漏洞統計

類別	確認數
1 SQL 注入	0
2 XSS	0
3 CSRF	1
4 越权	0（需 Bearer）
5 文件上傳/包含	0
6 RCE	0
7 敏感信息泄露	21
8 邏輯漏洞	0
合計	22

完整文件結構

```
/root/hexstrike-pentest/
├── PHASE2-FINDINGS.md
├── VULN-REPORT-8CATEGORIES.md
├── VERIFY-REPORT.md
├── WAF-BYPASS-VULNS.md
├── FINAL-REPORT.md
├── NAVIMOW-REPORT.md
├── LOOMO-NBO2O-WILLAND-REPORT.md       本文件
├── all-subdomains-connectivity.log
├── navimow-connectivity.log
├── recon/
│   ├── subfinder-{ninebot,segwayrobotics,loomo,nbo2o,navimow,willand}.com.txt
├── verify/
├── js-analysis/
│   ├── platform.bundle.js (599KB)
│   ├── sso-app.bundle.js (1.27MB)
│   └── nb-analysis/
│       └── fleet-umi.js (2.3MB) + 12 chunks
└── nuclei-results/
```

建議下一步

1. 重啟 fleet-api.ninebot.com 的後端服務 — 如果只是容器 crash，重啟就能完整測試 30+ saturn-portal 端點
2. 瀏覽器測試 navimow-bond 和 navimow-app-h5-dev — 看實際登入流程
3. navimow APP 真實 APK 下載 — 找 APK 鏡像
4. loomo.com SSL 確認 — 是否真的還在用？

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