ניתוח טכני פורנזי עמוק של מערכת ניהול התקני קצה, הפצת קושחה ומנגנוני תקשורת מבוססי Electron

הארכיטקטורה המורכבת של יישומי שולחן עבודה מודרניים דורשת שילוב הדוק בין יכולות מערכת הפעלה מקומיות לבין ממשקי משתמש מבוססי רשת. הניתוח הנוכחי בוחן מערכת ייחודית שפותחה על ידי חברת "א.ו. עולם של טכנולוגיה" (A.V. World of Technology), הפועלת תחת המותג ™WOT ומיועדת לניהול, עדכון וצריבת קושחה עבור מכשירים סלולריים, בדגש על פלח השוק של "טלפונים כשרים" המבוססים על ערכות שבבים של Spreadtrum/Unisoc.[1] המערכת מבוססת על שלד ה-Electron, המאפשר הרצת קוד JavaScript, HTML ו-CSS בסביבת Chromium, תוך שימוש ב-Node.js עבור פעולות בעלות הרשאות גבוהות במערכת ההפעלה.[3] ניתוח זה יסקור את מנגנוני התקשורת הפנימית (IPC), לוגיקת צריבת הרכיבים, אבטחת נכסים דיגיטליים, והחשיפות האבטחתיות במערכת התלויות (Dependencies) של היישום.

ארכיטקטורת המערכת ומנגנוני תקשורת בין-תהליכית (IPC)

יישומי Electron מפרידים מבנית בין תהליך ה-"Main", האחראי על הגישה למשאבי המערכת, לבין תהליכי ה-"Renderer", המנהלים את ממשק המשתמש. הגישור ביניהם מתבצע באמצעות מנגנון Inter-Process Communication (IPC). ביישום הנבדק, קובץ הליבה ipcConnection.js מגדיר את ערוצי התקשורת הראשוניים.[3] הקובץ נכתב במקור ב-TypeScript, כפי שמעידים ה-Helpers המיוצרים על ידי המהדר (__generator, __awaiter), מה שמצביע על תכנון מוקפד המיועד להבטיח טיפוסיות נתונים בסביבה המבצעת אינטראקציה עם חומרה.[3]

מבנה ערוצי ה-IPC ביישום מפורט בטבלה הבאה:

שם ערוץ ה-IPC	סוג פעולה	פונקציונליות ושימוש במערכת
basic-on-ipc	ipcMain.on	מאזין אסינכרוני המשמש לרישום לוגים וניטור אירועים המגיעים מה-Renderer.[3]
basic-handle-ipc	ipcMain.handle	מטפל (Handler) הניתן לקריאה בתצורת Invoke, המבצע בדיקות תקינות והחזרת ערכים לתהליך הממשק.[3]

השימוש ב-ipcMain.handle מעיד על אימוץ דפוסי פיתוח מודרניים המאפשרים לתהליך ה-Renderer להמתין (await) לתגובה מתהליך ה-Main, דבר הקריטי בעת ביצוע פעולות חומרה ארוכות הדורשות משוב מיידי על הצלחה או כישלון.[3]

ניהול מחזור חיים ועדכוני תוכנה אוטונומיים

היישום מטמיע מנגנון עדכונים אוטומטי המנוהל על ידי המודול autoUpdaterConnection.js המבוסס על חבילת electron-updater.[3] מנגנון זה חיוני בסביבה של צריבת קושחה, שבה כלי העבודה חייבים להיות מתואמים עם הגרסאות העדכניות ביותר של כלי הצריבה והדרייברים המופצים על ידי היצרן. הניתוח מעלה כי המערכת תומכת בלוקליזציה כפולת-שפה (עברית ואנגלית), כאשר קובץ המקור וקובץ ה-Map הנלווה מצביעים על תשתית רחבה יותר הכוללת גם תרגום לשפה האסטונית ("et").[3]

מצבי העדכון וההודעות המועברות למשתמש מתוארים להלן:

מצב עדכון	הודעה בעברית	פעולה אופרטיבית
checking-for-update	בודק עדכון	יצירת קשר עם שרת ה-Update וביצוע השוואת גרסאות.[3]
update-available	עדכון זמין	הורדת חבילת העדכון ברקע ללא הפרעה למשתמש.[3]
update-not-available	אין עדכון זמין	אישור כי המערכת פועלת בגרסה העדכנית ביותר.[3]
update-downloaded	עדכון הורד	הפעלת פונקציית quitAndInstall לסגירה ועדכון היישום.[3]
error	שגיאה בעדכון	תיעוד השגיאה ודיווח למערכת הניטור המרכזית.[3]

המעבר האוטומטי להתקנה (quitAndInstall) עם סיום ההורדה מצביע על מדיניות עדכונים כפויה (Mandatory Updates), המבטיחה כי כלל הסוכנים והמעבדות העובדים עם התוכנה ישתמשו בגרסה המסונכרנת עם השרתים המרכזיים של WOT.[1]

מנוע הצריבה והממשק לכלי ה-ResearchDownload

היכולת המרכזית של המערכת היא צריבת קושחה על מכשירים ניידים. פעולה זו מבוצעת באמצעות גישור בין יישום ה-Electron לבין כלי חיצוני מבוסס Windows בשם CmdDloader.exe.[3] כלי זה הוא גרסת שורת הפקודה של תוכנת ה-ResearchDownload המיועדת למעבדים מבית Unisoc/Spreadtrum.[2]

ניתוח פקודות ותהליך הרצת ה-Binary

קובץ ה-execCMDConnection.js אחראי על יצירת תהליך הבן (Child Process) והעברת הפרמטרים הנדרשים ל-CmdDloader.exe.[3] לפני תחילת הצריבה, המערכת מבצעת פעולת "ניקוי סביבה" על ידי מחיקת קובץ ההגדרות ResearchDownload.ini מספריית ה-Setting, מה שמבטיח כי הגדרות קודמות לא ישפיעו על

התהליך הנוכחי.[3]

הפרמטרים המועברים לכלי ה-Binary כוללים מידע רגיש והגדרות חומרה קריטיות:

דגל (Flag)	משמעות טכנית	מקור הנתונים
-p	סיסמה או טוקן גישה לצורך פתיחת הקובץ או אימות מול הכלי.[3]	מופק מטוקן הגישה של המשתמש.[3]
-v	גרסת ה-Binary או גרסת הפרוטוקול הנדרשת.[3]	מוגדר במערכת ה-Deployment.
-pid	מזהה מוצר (Product ID) הייחודי לדגם המכשיר.[3]	נבחר על ידי המשתמש בממשק.
-ezmode	מצב הפעלה מפושט (Easy Mode) המונע שגיאות תפעוליות.[3]	קבוע במערכת.
-port	זיהוי יציאת ה-COM אליה מחובר המכשיר הנייד.[3]	מזוהה אוטומטית על ידי המערכת.
-pac	נתיב מלא לקובץ הקושחה בתצורת PAC.[2]	נתיב ההורדה המקומי.[3]

ניתוח פורנזי של ה-CmdDloader.exe בסביבות ארגז חול (Sandbox) העלה ממצאים של "פעילות חשודה" בשל יכולתו להזריק קבצי הרצה (כמו uQe.exe) ולגשת להגדרות אבטחה של מערכת ההפעלה.[6] עם זאת, בהקשר המקצועי של צריבת טלפונים, התנהגויות אלו הן לרוב חלק אינטגרלי מהצורך של כלי הצריבה לתקשר עם דרייברים ברמה נמוכה (Low-level) ולבצע כתיבה לזיכרון ה-Flash של המכשיר.[6]

ניטור התקדמות ופענוח פלט בזמן אמת

היישום אינו מסתפק בהרצת הכלי, אלא מבצע ניטור (Parsing) רציף של ה-Standard Output (stdout) של תהליך ה-Binary.[3] המערכת משתמשת בביטויים רגולריים (Regex) כדי לחלץ נתוני אחוזים: /\ (\d+)%.[3] מידע זה מועבר בזמן אמת ל-Renderer כדי להציג למשתמש סרגל התקדמות.

בנוסף, המערכת מזהה מצבי כישלון או הצלחה ספציפיים המפורטים להלן:

- **הצלחה**: זיהוי המחרוזת Download Result = Passed; המפעיל את לוגיקת סיום ההתקנה וצריכת הקרדיטים.[3]
- **כישלון אימות**: זיהוי Invalid user המצביע על בעיית הרשאות מול השרת המרכזי.[3]
- **בעיות תקשורת**: זיהוי קודים כמו או המצביעים על כשל בפתיחת יציאת ה-COM, מה שמאפשר למערכת

להציע למשתמש ניסיון חוזר (Retry) במקום הודעת שגיאה סופית.[2]

אבטחת נכסים דיגיטליים ומנגנון הורדה מקוטע

קבצי הקושחה (PAC) הם קבצים בנפח גדול הדורשים מנגנון הורדה חסין ואמין. המודול fileDownloadConnection.js מטפל במשימה זו תוך שימוש באסטרטגיית הורדה מקוטעת (Chunked Download) מול שירותי אחסון בענן (S3).[3]

ארכיטקטורת ההורדה ותיוג הקבצים

כדי למנוע עומס על הזיכרון ולאפשר התאוששות משגיאות רשת, המערכת מבצעת את הפעולות הבאות:

1. **קבלת מטא-נתונים**: שליחת בקשת HEAD לשרת לקבלת ה-Content-Length המדויק.[3]
2. **חלוקה למקטעים**: ההורדה מתבצעת במקטעים של 5MB ($5 \times 1024 \times 1024$ בתים) תוך שימוש בדגל ה-Range בבקשות ה-HTTP.[3]
3. **הצפנה מקומית**: הקבצים נשמרים בסיומת .crypt בתיקיית ה-userData של המשתמש.[3] השימוש בטוקן מזהה כחלק משם הקובץ מבטיח כי לא ניתן יהיה להשתמש בקובץ הצריבה ללא אישור היישום, מה שמהווה נדבך מרכזי במודל העסקי של החברה.[3]

המערכת מחייבת כותרות (Headers) ספציפיות לצורך ביצוע ההורדה, מה שמונע גישה ישירה לקבצים מחוץ ליישום:

- Authorization: טוקן Bearer המזהה את המשתמש.[3]
- app-origin: מוגדר כ-desktop-app לצורך סינון בקשות ברמת ה-Firewall של השרת.[3]

המודל העסקי: לוגיקת צריכת קרדיטים מבוססת API

היישום משמש ככלי עסקי עבור מעבדות וסוכנים, ולכן הוא כולל מנגנון מובנה לגביית תשלום עבור כל פעולת צריבה.[1] לוגיקה זו מרוכזת בפונקציה המטפלת באירוע handle-install-end.[3]

ניתוח נקודות הקצה (Endpoints) וסביבות העבודה

המערכת פועלת מול שני ממשקי API בהתאם לסביבת ההרצה:

סביבה	כתובת API בסיסית	תפקיד
פיתוח (Dev)	http://192.168.50.76:8080/api	בדיקות פנימיות של לוגיקת צריכת הקרדיטים.[3]
ייצור (Prod)	https://dashboard.wot.co.il/api	השרת המרכזי המנהל את מאזן הקרדיטים של הסוכנים.[3]

עם סיום מוצלח של תהליך הצריבה על ידי ה-CmdDloader.exe, נשלחת בקשת POST לכתובת:

API_BASE_URL}/desktop/credits/consumeFile?access_token=${accessToken}.[3]}$

בגוף הבקשה נשלח ה-fileToken, המזהה את הקובץ הספציפי שנצרב.[3] זהו מנגנון קריטי המונע "צריבות פיראטיות"; גם אם המשתמש הצליח להשיג את קובץ ה-PAC, הכלי לא יאפשר את הצריבה ללא אישור מהשרת המרכזי של WOT, והסוכן יחויב בקרדיטים בהתאם לסוג המכשיר.[1]

הערכת סיכוני אבטחה וחשיפות במערכת התלויות

ניתוח של קבצי הרישיון וה-Source Maps חושף את מחסנית הטכנולוגיות (Tech Stack) של ממשק המשתמש, המבוססת על React v16.13.1 ו-React Router v6.26.0.[3] בחירה זו חושפת את היישום למספר פגיעויות אבטחה משמעותיות שהתגלו במהלך שנת 2025 וראשית 2026.

פגיעויות ב-React Router ו-Remix

גרסאות React Router v6.26.0 ו-@remix-run/router v1.19.0 נמצאו חשופות למספר וקטורי התקפה ברמת חומרה גבוהה.[9] הפגיעויות העיקריות כוללות:

מזהה CVE	חומרה (CVSS)	וקטור התקפה ותיאור
CVE-2026-22029	8.0 (High)	XSS דרך Open Redirect. מאפשר הרצת JavaScript זדוני בדפדפן דרך נתיבי ניווט לא מאובטחים.[11]
CVE-2025-59057	7.6 (High)	XSS ב-Meta APIs. חשיפה המאפשרת הזרקת סקריפטים דרך תגיות ld+json.[9]
CVE-2025-68470	6.5 (Medium)	הפניה לאתרים חיצוניים (Open Redirect) דרך נתיבים המתחילים ב-//.[13]
CVE-2026-22030	6.5 (Medium)	CSRF בבקשות POST למסלולי ממשק המשתמש בעת שימוש ב-Framework Mode.[10]

בסביבת Electron, פגיעות XSS היא קריטית במיוחד. אם תהליך ה-Renderer אינו מוגדר עם contextIsolation קשיח, תוקף המנצל XSS יכול להזריק קוד שיקרא ל-IPC המעניק גישה למערכת ההפעלה, ובכך להשיג שליטה מלאה על מחשב הסוכן (Remote Code Execution).[11]

חשיפות ברכיבי הליבה של React

אף ש-React v16.13.1 נחשבת לגרסה יציבה יחסית, המערכת עלולה להיות חשופה לפגיעות ה-RCE הקריטית שהתגלתה ברכיבי React Server Components (CVE-2025-55182, CVSS 10.0), במידה והיישום עושה

שימוש במנגנוני Decoding של ה-Payloads בצד השרת או ב-Node.js.[16] המלצת האבטחה הגורפת היא עדכון לגרסאות x.19 המכילות את התיקונים הנדרשים.[16]

ניתוח פורנזי של סביבת הריצה והנכסים המקומיים

המערכת מסתמכת על ניהול קבצים מקומי לצורך פעולתה התקינה. קבצי ה-Source Map מעידים על מבנה פרויקט הכולל הפרדה בין קוד ה-Main (הנמצא תחת /electron/) לבין קוד ה-Renderer (הנמצא תחת /src/).[3]

המבנה המקומי המזוהה כולל:

- cmd/CmdDloader.exe: כלי הליבה לביצוע הצריבה.[3]
- cmd/Setting/ResearchDownload.ini: קובץ הקונפיגורציה שמתנקה בכל הרצה כדי למנוע דליפת הגדרות בין מכשירים.[3]
- static/js/main.[hash].js: קובץ הממשק המגובב (Hashed) לצורך ניהול זיכרון מטמון יעיל. השימוש ב-Hash מבטיח כי בכל עדכון גרסה, הסוכן יוריד את הקוד העדכני ביותר.[18]

הקשר ל-"Nomad Surfers" שנמצא ב-Source Maps של קובץ ה-Main עשוי להעיד על שימוש חוזר בתבנית פרויקט (Boilerplate) או בנכסים דיגיטליים שמקורם במיקור חוץ, מה שעלול להוות סיכון אבטחתי אם לא בוצע ניקוי (Sanitization) מלא של הקוד לפני הפצתו לסוכני WOT.[3]

סיכום ומסקנות הניתוח

מערכת הניהול והצריבה מבית WOT היא פתרון טכנולוגי מתקדם המותאם אישית לשוק התיקונים והקושחה בישראל.[1] השימוש ב-Electron מאפשר גמישות גבוהה, אך דורש תחזוקה מתמדת של אבטחת רכיבי הצד-שלישי.

קטגוריית ממצא	סטטוס והשפעה	המלצות אופרטיביות
מנגנון צריבה	יעיל ומקצועי, מבוסס על הכלים הרשמיים של Unisoc.[2]	המשך שימוש ב-ezmode וניקוי ה-.ini למניעת שגיאות חומרה.[3]
אבטחת נכסים	הורדה מקוטעת ומוצפנת ברמה טובה מאוד.[3]	שקילת שימוש ב-Integrity Check (SHA-256) לפני הצריבה.
ניהול רישוי	מודל עסקי חסין המבוסס על אימות API וקרדיטים.[1]	הצפנת תעבורת ה-API ומניעת Man-in-the-Middle על טוקן הגישה.
חשיפות תלויות	**סיכון גבוה**. שימוש בגרסאות פגיעות של React Router החשופות ל-XSS.[9]	עדכון מיידי ל-React Router v6.30.2 לפחות.[10]

לסיכום, המערכת מפגינה רמת בשלות גבוהה בתחומי ה-DevOps והחומרה, אך זקוקה לשיפור משמעותי בהיבטי Application Security כדי להבטיח את הגנת הסוכנים והלקוחות הסופיים מפני מתקפות מבוססות רשת.[1] הניתוח הפורנזי של הקבצים מעלה כי מדובר בכלי רב-עוצמה שבידיים הלא נכונות עלול לשמש כוקטור תקיפה בשל הרשאותיו הגבוהות במערכת ההפעלה.[6]

עבודות שצוטטו

1. א.ו. עולם של טכנולוגיה | עולם שלם של טכנולוגיה וקידמה, נרשמה גישה בתאריך מאי 2, 2026 https://wot.co.il/
2. ResearchDownload User Guide - Insmat, נרשמה גישה בתאריך מאי 2, 2026 https://www.insmat.fi/files/share/K%C3%A4ytt%C3%B6ohjeet/ERIFON%204G%20DUKE%20P%C3%96YT%C3%84%20GSM%20%20MUSTA/Duke%204G%2003 2024%20P%C3%A4ivitys/ResearchDownload%20User%20Guide%20(en).doc
3. autoUpdaterConnection.js
4. ResearchDownload User Guide v1.0.7 | PDF | Flash Memory | Computer File - Scribd, נרשמה גישה בתאריך מאי 2, 2026 https://www.scribd.com/document/598209170/ResearchDownload-User-Guide-en
5. How to use spd flash tool to Update Any spreadtrum Android Mobile Firmware - YouTube, נרשמה גישה בתאריך מאי 2, 2026 https://www.youtube.com/watch?v=xvgkabuXYfA
6. Malware analysis 029028153dd7a5ef375bfafaf394cd5515c20118d79034ee8c1339d9c98ef135 Malicious activity | ANY.RUN, נרשמה גישה בתאריך מאי 2, 2026 https://any.run/report/029028153dd7a5ef375bfafaf394cd5515c20118d79034ee8c1339d9c98ef135/b38de677-bb8e-4842-b5de-3db13809d36b
7. How To Use Research or Upgrade Download Tool - YouTube, נרשמה גישה בתאריך מאי 2, 2026, https://www.youtube.com/watch?v=vIXylSwA_AY
8. react 16.13.1 - Snyk Vulnerability Database, נרשמה גישה בתאריך מאי 2, 2026 https://security.snyk.io/package/npm/react/16.13.1
9. Warning: High severity vulnerabilities in React Router, Patch Immediately! | CCB Belgium, נרשמה גישה בתאריך מאי 2, 2026 https://ccb.belgium.be/advisories/warning-high-severity-vulnerabilities-react-router-patch-immediately
10. Security Update: Multiple vulnerabilities in React Router and Remix - Netlify, נרשמה גישה בתאריך מאי 2, 2026 https://www.netlify.com/changelog/2026-01-15-react-router-remix-security-vulnerabilities/
11. CVE-2026-22029: React Router XSS Vulnerability - SentinelOne, נרשמה גישה בתאריך מאי 2, 2026 https://www.sentinelone.com/vulnerability-database/cve-2026-22029/
12. CVE-2025-59057 - Red Hat Customer Portal, נרשמה גישה בתאריך מאי 2, 2026 https://access.redhat.com/security/cve/cve-2025-59057
13. CVE-2025-68470 Detail - NVD, נרשמה גישה בתאריך מאי 2, 2026 https://nvd.nist.gov/vuln/detail/CVE-2025-68470
14. CVE-2025-68470: React Router Path Open Redirect - Miggo, נרשמה גישה בתאריך

2026 ,2 מאי, https://www.miggo.io/vulnerability-database/cve/CVE-2025-68470
15. CVE-2026-22030 : React Router is a router for React. In @remix-run/server-runtime version prior t - CVE Details, נרשמה גישה בתאריך 2 מאי 2026, https://www.cvedetails.com/cve/CVE-2026-22030/
16. Critical Security Vulnerability in React Server Components, נרשמה גישה בתאריך 2 מאי 2026 ,2, https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
17. Facebook React versions and number of CVEs, vulnerabilities, נרשמה גישה בתאריך 2 מאי 2026, https://www.cvedetails.com/version-list/7758/61450/3/Facebook-React.html?order=2
18. נרשמה גישה בתאריך 2 מאי 2026, https://create-react-app.dev/docs/production-build/#:~:text=Inside%20the%20build%2Fstatic%20directory,enables%20long%20term%20caching%20techniques.
19. Creating a Production Build - Create React App, נרשמה גישה בתאריך 2 מאי 2026, https://create-react-app.dev/docs/production-build/
20. react scripts build generate new hash even if the code not changes - Stack Overflow, נרשמה גישה בתאריך 2 מאי 2026, https://stackoverflow.com/questions/73601261/react-scripts-build-generate-new-hash-even-if-the-code-not-changes