

ניתוח אירוע השבתת שירותי GitHub Actions (פברואר 2026)

תקציר:


מה קרה: השבתה נרחבת של שירותי האוטומציה (Actions) ב-GitHub בעקבות תקלה אצל ספק תשתית (Upstream).

השורה התחתונה: האירוע מדגים את הסיכון הקריטי בניהול שרשרת אספקה דיגיטלית (Supply Chain Risk) ואת הצורך בתוכנית המשכיות עסקית (BCP) גם עבור כלים שנחשבים ל"סטנדרט התעשייה".

ציר זמן:

זיהוי ראשוני: בתאריך 02/02/2026 21:03 שעות ישראל (19:03 UTC).
התפתחות: זיהוי תקלה ב-Hosted Runners (השרתים שמריצים את העבודה).
סטטוס נוכחי: התקלה נפתרה ב-03/02/2026 בשעה 02:56 שעות ישראל (00:56 UTC).

February 2026



Incident with Actions

This incident has been resolved. Thank you for your patience and understanding as we addressed this issue. A detailed root cause analysis will be shared as soon as it is available.

Feb 2, 19:03 - Feb 3, 00:56 UTC

ניתוח סיכונים מזווית GRC:

זמינות (Availability): פגיעה ב-SLA של הארגון. האם הארגון יכול להרשות לעצמו עצירה של יותר מ-4 שעות בתהליכי הפיתוח?

סיכון צד ג' (Third-Party-Risk): התלות בספק יחיד (Single Point of Failure). מה קורה כשה-SaaS המרכזי שלך נופל?

אבטחה (פוגע ב-Integrity): שיבושים בשירותי ה-Dependabot וה-Copilot עלולים לעכב תיקוני אבטחה קריטיים לקוד הארגוני.

מטריצת השפעה:

משמעות עסקית	רמת השפעה	תחום מושפע
עצירה מוחלטת של גרסאות חדשות	גבוהה	פיתוח (R&D)
עיכוב בסריקת חולשות אוטומטית	בינונית	אבטחת מידע
חוסר יכולת לבצע התאוששות מאסון (DR)	קריטית	תפעול (Ops)

המלצות לשיפור:

גיוון ספקים: שימוש ב-Self-hosted-runners (שרתים מקומיים) למשימות קריטיות, כדי לא להיות תלוי ב-100% בענן של GitHub.

עדכון נהלי חירום: הגדרת צהליך ידני לשיגור גרסאות קריטיות בזמן תקלת ענן.

ניטור ובקרת ספקים: הגדרת התראות אוטומטיות על סטטוס הספקים (Status Dashboard monitoring).