Google

אבטחת הבסיס לפיתוח תוכנה

לנוכח העלייה הדרמטית בגורמים זדוניים באינטרנט ובמתקפות סייבר במימון מדינות, אנחנו מאמינים שאבטחת המוצרים והשירותים שלנו חשובה לא פחות מיעילותם. אנחנו ב-Google ממוקדים כיום יותר מאי פעם בהגנה על אנשים, ארגונים וממשלות, על ידי שיתוף המומחיות שלנו, העצמת החברה לטיפול בסכנות הסייבר המתפתחות מהר מתמיד וקידום שוטף של אבטחת סייבר ברמה הגבוהה ביותר, במטרה ליצור עולם בטוח יותר לכולם.

תוכנה בקוד פתוח – קוד שכולם יכולים להשתמש בו, לשנות אותו ולהשתמש בו כבסיס לפיתוח בחינם – היא הבסיס לאינטרנט המודרני. בזכות שיתוף פתרונות תוכנה בקוד פתוח, אנשים יכולים לשתף פעולה והחדשנות מואצת. עם זאת, אותה פתיחות שהופכת את העולם הדיגיטלי לנגיש לכולם היא גם מה שהופכת אותו לחשוף לאיומי אבטחה.

האתגר

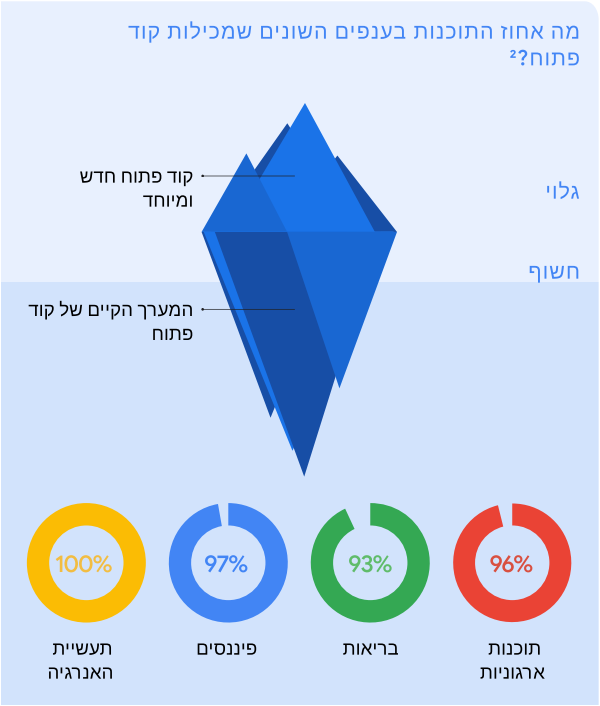
תוכנה בקוד פתוח היא בעיה של כולם

קהילת המפתחים בקוד פתוח נשענת על שקיפות ושיתוף, תוך תרומת כמויות אדירות של קוד לרוב האפליקציות שבהן אנחנו משתמשים כיום. אנשים נעזרים בתוכנות בקוד פתוח מדי יום ביומו, כמעט בכל רגע נתון – מציוד רפואי ועד לרשתות חשמל – מה שהופך פרויקטים בקוד פתוח לכר פורה למתקפות סייבר. בשלוש השנים האחרונות חלה עלייה של 742% משנה לשנה[1] במספר המתקפות על שרשרת אספקת התוכנה.

המערכת שעומדת בבסיס הקוד הפתוח מורכבת משכבות על גבי שכבות, שבהן יחסי תלות עקיפים וסמויים יכולים להכיל נקודות חולשה באבטחה. בגלל המורכבות של אותן שכבות קשה לאתר את נקודות החולשה ידנית, ואבטחת החלק הזה בתהליך פיתוח התוכנה הפכה לבעיית אבטחה דחופה בכל העולם.

צריך לרכז יותר את המאמצים בכל הרמות השונות:

- מפתחי תוכנות בקוד פתוח צריכים ידע ומשאבים כדי לאבטח את הפרויקטים שלהם.
- ארגונים צריכים להבין מהן הסכנות ונקודות החולשה בשרשרת האספקה כדי לפתח תוכניות טיפול.
- ממשלות והגורמים המובילים בתחום צריכים לחבור זה לזה כדי לפתח תקני אבטחה חזקים ויעילים[3].



[2] מקור מידע: Synopsys Open Source Security and Risk Analysis Report 2022

הפתרון שלנו

אבטחת תוכנות בקוד פתוח למען כולם

אנחנו ב-Google עובדים על פתרון הבעיה במשך שנים. למעשה, מדי שנה 10% מהגוגלרים תורמים לפרויקטים של תוכנות בקוד פתוח. המומחיות שלנו הובילה אותנו למסקנה שבעולם הדיגיטלי המודרני האבטחה יכולה להתקיים דווקא בזכות אימוץ הפתיחות. בזכות הגישות הפתוחות אנחנו יכולים לאמץ מהר את החידושים האחרונים ולאפשר ליותר אנשים לפתור אתגרי אבטחה. אבל כדי לממש את מלוא הערך שטמון בקוד פתוח, אנחנו צריכים שותפויות חזקות יותר בין המגזר הפרטי והציבורי, ומסגרות מדיניות דינמיות לתמיכה באבטחה למען כולם. לכן אנחנו שמחים על מאמצי הממשל האמריקאי לקידום האבטחה של תוכנות בקוד פתוח, כמו חוק האבטחה של תוכנות בקוד פתוח שהוגש לסנאט ב-2022.

- בעזרת מסגרות אבטחה מתקדמות, כמו רמות של שרשרת אספקה לארטיפקטים של תוכנה (SLSA)[5,4] ופיתוח כלי אבטחה מתקדמים, אנחנו עומדים בראש הקהילה.
- פיתחנו את הגרף להבנת הרכב הארטיפקטים (GUAC), שמשלב ידע הקשור לאבטחת תוכנה ממקורות שונים במסד נתונים יחיד, שעליו אפשר להריץ שאילתות. בזכות GUAC נשמרות החירויות – לכל ארגון יש גישה חופשית למידע הקשור לאבטחה ויכולת להשתמש בו.

המחויבות שלנו:

- להשקיע 100 מיליון דולר באבטחת קוד פתוח, לשמש בתפקידי ניהול בקרן לאבטחת קוד פתוח ולהוביל שיתוף פעולה בין המפתחים.
- להתוות ולשתף תקני אבטחה ישימים, הדרכות, כלים חופשיים ונהלים פנים-ארגוניים עם כלל קהילת הקוד הפתוח.
- לקדם זיהוי, כלים אוטומטיים לטיפול ודרכים ליצירת אבטחה בשלבי הפיתוח המוקדמים ביותר.
- ליצור כלים אוטומטיים כדי להפוך את האבטחה ברמת הארגון לחופשייה ונגישה לכולם.

אפליקציות

Google OSS-Fuzz
התגובה שלנו לבאג Heartbleed

הבאג Heartbleed היה נקודת חולשה חמורה בקוד פתוח, בעלת פוטנציאל להשפיע כמעט על כל אחד מהמשתמשים והמשתמשות באינטרנט. ב-2014, האקרים גנבו את השמות, הכתובות, תאריכי הלידה, מספרי הטלפון ומספרי תעודות הזהות של מטופלים ממאגר המידע של אחד מבתי החולים הגדולים בארה"ב.

בתגובה, Google השיקה שירות חינמי לקהילה בשם OSS-Fuzz. באמצעות הבדיקות של Fuzz אפשר להצביע על נקודות חולשה ידועות באבטחה תוך דקות, בניגוד לבדיקה ידנית שיכולה לקחת חודשים. השקענו ביצירת תשתית לבדיקה אוטומטית של מאות פרויקטים בקוד פתוח. כיום, בעזרת OSS-Fuzz נערכות סריקות שוטפות לקוד, והשירות כל הזמן משתדרג כדי לאפשר לזהות סוגים נוספים של באגים.

יותר מ-800 פרויקטים קריטיים בקוד פתוח נסרקים באמצעות Fuzz בשש שפות שונות.

ההשקעות ואבני הדרך שלנו בתחום

2020

אוגוסט
הצטרפות לקרן לאבטחת קוד פתוח (OpenSSF) כדי להנחות ולשפר את האבטחה של תוכנות בקוד פתוח.

2021

מאי ויוני
הקמת נהלים מומלצים לאבטחת קוד פתוח בהתאם לצו הנשיאותי של הבית הלבן 14028 ומתן הדרכה בנוגע לתקני אבטחה בשרשרת אספקת התוכנה.

יוני
הפצת SLSA באמצעות OpenSSF – חשיפת מסגרת האבטחה הפנימית של Google כדי לאפשר לכולם ליצור תוכנות מאובטחות יותר.

אוגוסט
התחייבות להשקעת 100 מיליון דולר בקידום ובאבטחה של תוכנות בקוד פתוח, כולל חבירה למפתחים כדי לזהות ולתקן נקודות חולשה.

2022

מאי
השקת צוות התחזוקה של Google לקוד פתוח במסגרת כנס בוושינגטון DC – צוות של מפתחים במשרה מלאה שמקדישים את עבודתם ישירות לפרויקטים בקוד פתוח, במטרה לשפר את אבטחתם.

מאי
השקת המוצר Assured Open Source Software, שעוזר לשלב את אותן חבילות מהימנות בקוד פתוח שבהן Google משתמשת בתהליכי פיתוח.

נהלים מומלצים של Google שיכולים לעזור לארגונים ציבוריים ופרטיים לשמור על האבטחה כיום:

- להשתמש ב-SLSA כדי להקשיח את האבטחה של שרשרת אספקת התוכנה
- לזהות, לעקוב ולטפל בנקודות חולשה בדרכים אוטומטיות באמצעות OSS-Fuzz ו-OSV.dev
- להשתמש בחתימה קריפטוגרפית ולאמת את התוכנות באמצעות Sigstore
- להשתמש בכרטיסי מידע כדי להעריך אוטומטית סיכוני אבטחה ביחסי התלות

הגישה שלנו

חוזק התוכנה נקבע לפי חוזקה של החוליה החלשה ביותר. אנחנו משקיעים את המומחיות והמשאבים הכספיים שלנו בקידום האבטחה של כלל קהילת הקוד הפתוח. צוותי הפיתוח ומומחי האבטחה שלנו מאמינים שאנחנו יכולים להגן על יותר ארגונים ציבוריים ופרטיים בדרכים הבאות:

הצוות שלנו בוחן כל שלב במחזור החיים של המוצר, וסורק, מנתח ובודק אותו באמצעות Fuzz כדי לזהות נקודות חולשה.

אנחנו תומכים באינטרנט הפתוח ומשתפים את הידע שלנו עם קהילת המפתחים, כדי לשמור על אבטחת הציבור והעסקים.

אנחנו מזהים איומים מתוחכמים, מספקים כלים אוטומטיים מתקדמים ומקדימים תרופה למכה כדי לשמור על האבטחה גם מפני סכנות חדשות בעתיד.

אבטחת תוכנות בקוד פתוח נשענת על שיתוף אחראי, ואנחנו מחויבים לשיתוף פעולה שוטף סביב הבעיה הדחופה והקריטית הזו. g.co/security/gosst

מקורות מידע: 4. בזכות שיתוף הידע שלנו (כלומר, הפצת SLSA והובלת OpenSSF), כל מי שיוצר תוכנה, לא רק Google, יכול ליהנות מהמומחיות ומנוהלי האבטחה של Google שעמדו במבחן הזמן. 5. SLSA היא מסגרת של עקרונות שיכולה לעזור לארגונים לשפר את האבטחה של תהליכי פיתוח התוכנה. היא עוזרת לעמוד בדרישות של ממשלת ארה"ב, כפי שהן הותוו במסגרת לפיתוח תוכנות מאובטחות כמענה לצו הנשיאותי בנושא אבטחת סייבר. בעזרתה הארגונים יכולים לציית להנחיות הפדרליות וליצור תוכנות מאובטחות יותר למען כולם.