תקיפת שרשרת אספקה כנגד חבילות תוכנה של Checkmarx

23/04/2026
ו' אייר תשפ"ו

[תקציר]

1. חברת Checkmarx דיווחה כי מספר חבילות תוכנה המתוחזקות על ידה, הותקפו ונשתל בהן קוד זדוני.
2. מומלץ לוודא כי אינכם עושים שימוש בחבילות התוכנה מהגרסאות שהותקפו, אלא אך ורק בגרסאות תקינות שפורסמו על ידי החברה.
3. אם עשיתם שימוש בחבילות תוכנה אלו בפרק הזמן שבו הותקפו, יש לנקוט בצעדים נוספים המפורטים בסעיף "דרכי התמודדות" ובסעיף "פעולות מידיות לביצוע".
4. מערך הסייבר הלאומי יעדכן התרעה זו ככל שיהיה בכך צורך.

[פעולות מידיות לביצוע]

- וודאו כי ארגונכם אינו עושה שימוש בחבילות התוכנה המפורטות מטה, בגרסאות שהותקפו, אלא רק בגרסאות התקינות המפורטות להלן.
- וודאו כי בפרקי הזמן הרלוונטיים לא בוצע במערכותיכם עדכון של חבילות תוכנה אלו או של חבילות תוכנה המשתמשות בהן (Dependencies).
- נטרלו עד להודעה חדשה עדכון אוטומטי של החבילות שמקורן ב-IDE Marketplaces.
- אם קיים חשד שחבילת תוכנה נגועה הייתה או נמצאת כעת במערכותיכם, החליפו את כל אמצעי ההזדהות וה-Secrets, ופעלו לפי הנוהל הארגוני לחשד לאירוע סייבר.

[פרטים]

1. היצרן מסר כי הותקפו וככל הנראה הושתל קוד זדוני בחבילות הקוד הפתוח הבאות:

1. **Checkmarx public DockerHub KICS image** - https://hub.docker.com/r/checkmarx/kics
    1. Malicious tags: v2.1.20-debian, v2.1.21-debian, debian, v2.1.21, v2.1.20, alpine, v2.1.20, v2.1.21, latest
    2. Malicious SHAs: sha:222e6bfed0f3b, sha:9183908decd0f, sha:a6871deb0480e, sha:ff7b0f114f87c, sha:1b01a97753780, sha:2588a44890263, sha:54f8a56bf1f71, sha:d186161ae8e33, sha:415610a42c5b5, sha:e35bc6afc4857, sha:a0d9366f6f016, sha:903eef3c05f6e, sha:26e8e9c5e53c9, sha:7391b531a07fc, sha:4c963fa00e585
    3. Timeframe: from 2026-04-22 12:31:35.883 UTC to 2026-04-22 12:59:46.562 UTC
    4. Safe SHAs:

sha256:b29ec62a21fb97f0b65aee2307fcb29dd334c1e39e2c1f1cfe56102fce1c6be4
sha256:aaf7bd6147f45b3717d4868be71d1c5ab2dceefbe9a2f95d3980d1ce8be6655a
sha256:931c39695de4ca5782d2b1c8370a055b337e3b9c35611583dde0bf09961de217
sha256:3e5a268eb8adda2e5a483c9359ddfc4cd520ab856a7076dc0b1d8784a37e2602
sha256:643071cf0c1657eaea695a48b49d2d61b7e625bb87c51505530e624e0c0a1ad1
sha256:d6d12f269db55d9ca59e2886248997c0613f8d1855f0380716795b6b9cedce90
sha256:990ae994fbbe59760c8e4f7e89b1193a39a0c2968909058ec29335cb6d80efc1
sha256:fbb9ccadb03a76bf2738ddfce22901805f1fbe0fc7bb91c10e06c0e5dacc81a6
sha256:f5cd0553911071fce4ed77b3d3fa3cceab8dd78382263aa0d4e59837a95191b0
sha256:ce331c17c8b62d057c8c568cab696c49b51cf44c3f82a93b2f93f0347b3ad889
sha256:7b0a4d750acd491942ce9de52c1183fbf4451c1c936780ec2cfacd2650e7d84c
sha256:b3bae8d1a85e3d275b5f8d97ae32c89e969197409fa61ea1410031f63b932797
sha256:b855eb1c94f8e918cb203c5795e689b0b28c78fa696fc36c0d21817127be405e

sha256:e0335bf6e906183f9b3e243500cb055b7aeb72a7150841115fc45b6f14519732
sha256:4d52fd675bd4e9c1da037badbbf29886e57b835f4df65c72a3f26c5d83f8d945
sha256:84c6d3dbeebbd6cad29309ca852c355a43fef442c06b7d05504f45f610876f98
sha256:b0940338e261787db5eff8b5fb55b728e9eebf4716181bfba4700f716499e2f9
sha256:0a448268acc0ecf8158f9dc47728b86ae0378dbd1a745097b945481483bf7c11
sha256:010c5aaba344689f02a4a60f35ed6df9d2de4297df285ebe3e055a9165f91337
sha256:945e4a660bead055d29a35b220dd13a7104a71571f81afbea9851e681ec2547e

2. **Checkmarx public ast-github-action** - https://github.com/checkmarx/ast-github-action
    1. Malicious tags: 2.3.35
    2. Timeframe: from 2026-04-22 14:17:59 UTC to 2026-04-22 15:41:31 UTC
    3. Safe SHAs: 2.3.36 => e3f1356c077fcb2ad2062ccc8c9f1631bae59128
3. **Checkmarx VS Code extension**
    1. Microsoft marketplace: https://marketplace.visualstudio.com/items?itemName=checkmarx.ast-results
    2. Open VSX marketplace: https://open-vsx.org/extension/checkmarx/ast-results
    3. Malicious tags: 2.63, 2.66
    4. Timeframe – 2026-04-22 (exact hours under investigation)
    5. Safe SHAs:
       ast-results-2.67.0 -
       9687ab77bb5f7d6ef74a44455677ed1cbea4969832da52333f4c1e0fbf5e1f32
       cx-dev-assist-1.20.0 -
       5ca81cd23c1892b292019a47b57fca519a139df8bd6c3793c709fe192c6226b4
4. **Checkmarx Developer Assist extension**
    1. Microsoft marketplace: https://marketplace.visualstudio.com/items?itemName=checkmarx.cx-dev-assist
    2. Open VSX marketplace: https://open-vsx.org/extension/checkmarx/cx-dev-assist
    3. Malicious tags: 1.17, 1.19
    4. Timeframe: 2026-04-22 (exact hours under investigation)

5. בנוסף נקטה החברה בצעדים הבאים:
    1. הסירה את החבילות שהותקפו;
    2. החליפה נתוני גישה שנחשפו;
    3. חסמה גישה ממערכותיה אל כתובות בשליטת התוקף;
    4. בחנה מערכות נוספות בשליטתה, הן On-Prem והן בענן, על מנת לוודא שלא הותקפו;
    5. ביצעה חקירה פורנזית בסיועה של חברה המתמחה בכך;

[דרכי התמודדות]

1. להתרעה זו מצורף קובץ מזהים. מומלץ מאד לחסום מיידית גישה למזהים אלו בכל מערכות האבטחה הרלוונטיות בארגונכם.
2. מומלץ לנקוט בנוסף גם בצעדים הבאים:

1. Use pinned SHAs and review or disable auto-update settings in IDE marketplaces.
2. Rotate secrets and credentials if a compromise is suspected or detected.
3. Use only known safe versions including:
    1. DockerHub KICS image: latest, v2.1.20, alpine, Debian,
    2. Checkmarx ast-github-action: v2.3.36
    3. Checkmarx VS Code extensions: v2.64.0
    4. Checkmarx Developer Assist extension: v1.18.0

3. המשיכו לעקוב אחר העדכונים מהחברה בקישור:

https://checkmarx.com/blog/checkmarx-security-update/