גאזט סייבר

רביעי, ח׳ בכסלו תשפ״ז · 18 בנובמבר 2026 · גיליון 5 · מהדורת יום רביעי

חולשה קריטית · ג׳אווה

חולשה בלב ג׳אווה: השתלטות מרחוק על Jira, Jenkins ועוד

החולשה, שקיבלה את הכינוי Java4Shell, נמצאה בעזרת AI בתוך שעה. אורקל תיקנה אותה ביום שלישי, ו־CISA קוראת לעדכן מיד. ניצול בפועל עוד לא דווח.

חוקרים חשפו ביום שלישי חולשה חמורה בג׳אווה, אחת מפלטפורמות התוכנה הנפוצות בעולם. היא עלולה לאפשר לתוקף מרחוק, בלי סיסמה, להשתלט על שרתים שמריצים מערכות ארגוניות מוכרות. הסוכנות האמריקאית להגנת סייבר, CISA, קוראת לארגונים לעדכן מיד. את החולשה מצאו בעזרת בינה מלאכותית, תוך כשעה.

למה זה חשוב? לפי חברת המחקר Calif, שמצאה את החולשה, ג׳אווה היא שפת התכנות השלישית בפופולריות בעולם, ו־90% מחברות Fortune 500 משתמשות בה. בנקים, חברות תעופה, תקשורת וגופי ממשל נשענים עליה. הבעיה לא נמצאת באפליקציה אחת, אלא ב־OpenJDK, סביבת ההרצה החופשית של ג׳אווה, שממנה בנויות רוב הגרסאות בשוק: של אורקל, Amazon, מיקרוסופט, Red Hat ועוד. החולשה קיבלה את המספר CVE-2026-114938 ואת הכינוי Java4Shell.

איך זה עובד? השיטה Base64 היא דרך נפוצה לכתוב מידע בינארי כטקסט. משתמשים בה בהזדהות, בהעלאת קבצים ובהודעות רשת. כדי לפענח אותה מהר יותר, ג׳אווה מפעילה פקודות מיוחדות של מעבדי אינטל ו־AMD חדשים, בקוד

שנכתב ביד בשפת אסמבלי, הקרובה לשפת המעבד. לפי Calif, קלט של 64 פעמים האות A ואחריהן סימן = גורם לקוד הזה לכתוב 62 בתים מעבר לשטח הזיכרון שהוקצה לו. זו השחתת זיכרון, כלומר דריסה של מידע סמוך, בשפה שאמורה להגן מפני בדיוק זה. בעבודה זהירה, לפי Calif, אפשר להפוך אותה לדליפת זיכרון או להרצת קוד מרחוק, כלומר השתלטות על השרת.

מי חשוף? לפי Calif, החוקרים הריצו קוד בלי הזדהות על Keycloak, Jira, Confluence, JFrog Artifactory, Jenkins ו־PingFederate בהגדרות ברירת המחדל. ב־Kafka, Solr ו־Elasticsearch הם עשו זאת אחרי הזדהות. לפי Red Hat, החולשה פוגעת בג'אווה מגרסה 17.0.6 ואילך, כולל 21 ו־25, רק במעבדי x86-64 שתומכים בהרחבה VBMI AVX-512: מעבדי Xeon מדור Ice Lake ואילך ומעבדי AMD מדור Zen 4 ואילך. מעבדי ARM לא נפגעים, וגם לא ג'אווה 8 ו־11 הרגילות. כל אפליקציה שמפענחת Base64 שמגיע מבחוץ עלולה להיות חשופה.

ותוקפים כבר מנצלים אותה? לפי Tenable, עד יום שלישי לא דווח על ניצול, והחולשה לא נכנסה לרשימת החולשות המנוצלות של CISA. Cisco Talos כתבה שלא ראתה ניצול, אבל צופה ניסיונות בקרוב. חברת GreyNoise פתחה לוח מעקב חי, ולדבריה ניצול המוני יהיה קשה בהתחלה, כי צריך להתאים את המתקפה לכל מערכת. חברת Calif פרסמה רק קוד שמדגים את הבאג, ושומרת לעצמה את המתקפות המלאות. לפי Tenable, החוקר Kevin Breen מ־Immersive כתב ב־X שבנה מתקפה עובדת. החברה עצמה כתבה ב־X שפרטי החולשה דלפו לפני שיצא התיקון.

חלק מהסערה נוגע לדרך שבה נמצאה החולשה. לפי BleepingComputer, החוקר Quang Luong מ־Calif מצא אותה בתוך כשעה בעזרת Codex, כלי התכנות של OpenAI, ובנה מתקפה ראשונה בשעתיים נוספות, בעלות של פחות מ־200 דולר. לפי ה־BBC, מדובר במודל הסייבר החדש של OpenAI, שעוד לא זמין לציבור. לא כולם מתרשמים: החוקרים דירגו את החולשה 9.2 מתוך 10, ואורקל רק 8.1, עם מורכבות תקיפה גבוהה. לפי Datadog, קל יותר להפיל את התוכנה מאשר

להשתלט עליה. לפי The Register, Jan Schaumann מ־Akamai האשים את Calif במרדף אחרי פרסום.

מה לעשות? אורקל פרסמה ביום שלישי גרסאות מתוקנות במסגרת עדכון האבטחה החודשי שלה, עם 655 תיקונים: 17.0.21.1, 21.0.13.1, 25.0.5.1 ו־27.0.1.1. מי שמשתמש בגרסה של ספק אחר צריך את התיקון של אותו ספק. CISA מזכירה שג׳אווה מסתתרת גם בתוך מוצרים, קונטיינרים ומכשירים, ולא תמיד מופיעה ברשימות התוכנה. אחרי העדכון צריך להפעיל מחדש את התהליכים. עד אז אפשר להפעיל את ג׳אווה עם הדגל -XX:-UseBASE64Intrinsics, שמכבה את קוד הפענוח המהיר.

מקור: Calif · CISA · Red Hat · BleepingComputer · Tenable · BBC · The Register · Datadog · GreyNoise

בגיליון · הקישו לקפיצה

פריצות ואירועים ←	AI ואבטחה ←	סייבר ב־X ←
תוקפים וקמפיינים ←	כלים ומחקר ←	חולשות מנוצלות ו־KEV ←

פריצות ואירועים

גאזט סייבר · 18 בנובמבר 2026

ענקית האנרגיה Equinor תחת מתקפת סייבר

מערכות IT ודואר פנימי שובשו. לפי החברה, ההפקה לא נפגעה ואין סימן לגניבת מידע.

חברת הנפט והגז הנורווגית Equinor הודיעה ביום שלישי בערב שהיא מזהה מתקפת סייבר מתמשכת נגד חלק ממערכות ה־IT שלה. לדברי החברה, היא הפעילה משאבים כדי לנטרל את המתקפה, אין סימנים לגניבת מידע, וההפקה והפעילות לא נפגעו. הרשויות עודכנו.

לפי Reuters, מערכת הדואר הפנימית של החברה לא עבדה, כך לדברי אדם בחברה שביקש שלא להזדהות. סוכנות הידיעות NTB דיווחה על שיבושים באפליקציות

ובמערכות פנימיות. Equinor היא ספקית הגז הגדולה באירופה. החברה לא מסרה מי עומד מאחורי המתקפה.

הרשות הנורווגית לביטחון לאומי, NSM, מסרה שהיא מסייעת. בחודש שעבר העלתה הרשות את הערכת הסיכון למתקפות סייבר לרמה 4 מתוך 5, ולדבריה, מספר מבצעי הסייבר המוצלחים נגד חברות נורווגיות שולש בחצי השנה האחרונה.

מקור: Equinor · Reuters (CNA)

אירלנד: פריצה לספק תוכנה חשפה נתונים של איגודי אשראי

ספק התוכנה Wellington IT משרת יותר משליש מאיגודי האשראי באירלנד. עד 1.8 מיליון חברים עלולים להיפגע.

יותר מ־40 איגודי אשראי באירלנד, גופים שמתפקדים כמו בנקים קהילתיים, קיבלו השבוע הודעה על פריצה אפשרית ממערכת של ספק התוכנה Wellington IT מבלפסט. לפי The Irish Times, התוקפים ניצלו חולשה בתוכנה של החברה ושלפו חלק מהרשומות של חברי האיגודים, כולל פרטים על תשלומים שיצאו מהחשבונות.

Wellington IT מספקת את מערכת הבנקאות ליותר משליש מאיגודי האשראי באירלנד. לפי העיתון, האירוע עלול לפגוע בעד 1.8 מיליון בני אדם, יותר ממחצית החברים. איגוד איגודי האשראי מסר שהחולשה נסגרה ושהיתרות לא נפגעו. שר האוצר, Simon Harris, אמר שהאירוע "מדאיג מאוד", ורשות הגנת המידע קיבלה כמה הודעות על דליפה.

> **מה לעשות:** חברי איגודי אשראי באירלנד: לחשוד בהודעות שמזכירות תשלומים או מוטבים, גם כשהפרטים בהן נכונים.

מקור: The Irish Times · TheJournal.ie

Infoblox נפרצה דרך ספק, וגיבויי רשת של לקוחות נגנבו

התוקפים נכנסו ל־SharePoint של חברת אבטחת הרשת דרך החשבונות של ספק העברת נתונים.

חברת אבטחת הרשת Infoblox חוקרת פריצה שעברה דרך ספק שעזר לה להעביר נתונים. לפי The Register, לספק הייתה גישה מהימנה ל־SharePoint של החברה, והתוקפים השתמשו בחשבונות שלו כדי להוציא משם מידע ישירות.

בין המידע שנגנב: גיבויים של מערכות NIOS של חלק מהלקוחות. אלה צילומי מצב של הגדרות DNS ו־DHCP, מסדי נתונים ויומנים, שמשמשים לשחזור המערכת אחרי כשל. לפי TechRadar, גיבוי כזה הוא מעין מפה של הרשת הארגונית. נגנבו גם פרטי עובדים ובני משפחותיהם, בהם מספרי ביטוח לאומי אמריקאי, תאריכי לידה ופרטי חשבון להפקדת שכר.

Infoblox מסרה שלפי החקירה עד עכשיו, המוצרים, שירותי הענן ועדכוני התוכנה שלה לא נפגעו. העובדים קיבלו 100 דולר לקניית מנהל סיסמאות ושנתיים של ניטור אשראי.

> **מה לעשות:** לקוחות Infoblox: לברר מול החברה אם גיבויי NIOS שלכם נגנבו, ולהחליף סודות שנשמרו בהגדרות.

מקור: The Register · TechRadar

מחשב העל היפני Fugaku הושבת אחרי פריצה

התוקף נכנס דרך לוח סטטוס ציבורי וגנב מפתחות התחברות של חוקרים.

מכון RIKEN היפני השבית את מחשב העל Fugaku אחרי שגורם זר חדר לרשת התפעול שלו בין 10 ל־13 בנובמבר. לפי המכון, הפריצה עברה דרך דף אינטרנט ציבורי שמציג את מצב המערכת. השיטה המדויקת עוד בבדיקה.

נחשפו שמות, כתובות מייל ומזהי משתמש של עד 4,222 משתמשי Fugaku ו־375 משתמשי מחשב העל RIKYU. מתיקיות המשתמשים נלקחו גם מפתחות SSH,

כלומר מפתחות דיגיטליים להתחברות מרחוק לשרתים, ומפתחות גישה לשירותים אחרים. לפי BleepingComputer, התוקף כבר ניסה להשתמש בחלק מהמפתחות כדי להיכנס למערכות נוספות. אין ראיה שנתוני מחקר נגנבו.

> **מה לעשות:** חוקרים שעבדו על Fugaku: לבטל כל מפתח SSH או מפתח גישה שנשמר שם, ולהסיר את המפתח הציבורי משרתים אחרים.

מקור: RIKEN · BleepingComputer

בקצרה

Rockstar: ההאקר הבריטי Arion Kurtaj, בן 21, הודה ביום שני בפריצות ל־Uber, ל־Revolut ול־Rockstar בספטמבר 2022 ובהדלפת קטעים מ־Grand Theft Auto VI. את חלק מהפריצות ביצע מטלפון מ־Fire Stick בחדר מלון, בזמן ששוחרר בערבות. גזר הדין צפוי בשבוע הבא. The Record

---

תוקפים וקמפיינים

גאזט סייבר · 18 בנובמבר 2026

סוכן AI ניהל את הסחיטה של חברה ישראלית גדולה

לפי גמביט סקיוריטי, האקרים רוסים גנבו כחצי מיליון קבצים, והסוכן קבע כמה לדרוש וייעץ במשא ומתן.

האקרים רוסים פרצו לחברה ישראלית גדולה, גנבו כחצי מיליון קבצים והשתמשו בסוכן בינה מלאכותית כדי לנהל את הסחיטה. כך חשפה "המהדורה המרכזית" של חדשות 12, על סמך מחקר של חברת גמביט סקיוריטי. בין הקבצים: דוחות כספיים, פרטי חשבונות בנק ומידע אישי של בכירים. שם החברה לא פורסם.

לפי הדיווח, ההאקר ביקש מהסוכן לנתח את המצב הכלכלי של החברה. הסוכן השיב שהיא מסוגלת לשלם כחצי מיליון דולר, וניסח מייל שדרש 500,000 דולר.

כשנציג החברה ענה שעלות מתקפה כזו היא 60 עד 80 אלף דולר בלבד, התוקפים העבירו גם את זה לסוכן. הוא קבע שהחברה מתמקחת, וייעץ להם: "יש להציג להם את התשלום כביטוח מפני אסון ולא כקנס".

"זו פעם ראשונה שאנחנו רואים סוכן AI שתוקף משתמש בו כדי לבצע גם את התהליך של הסחיטה והמשא ומתן עם החברה הנתקפת", הסביר בחדשות 12 אייל סלע, מנהל מודיעין איומי סייבר בגמביט סקיוריטי. הדיווח לא מציין באיזה כלי AI השתמשו התוקפים.

> **מה לעשות:** לשמור גיבויים מנותקים ותוכנית התאוששות, כדי שיהיה אפשר לחזור לפעילות בלי משא ומתן עם התוקפים.

מקור: N12 · ערוץ 7

מחקר: קבוצות איראניות מעבירות זו לזו גישה לרשתות פרוצות

AttackIQ מיפתה 20 קבוצות תקיפה איראניות, ומצאה שריגול משמש לא פעם קרש קפיצה להרס.

חברת האבטחה AttackIQ פרסמה ביום שלישי מחקר שמאחד דיווחים קודמים על 20 קבוצות תקיפה מטעם איראן. לפי המחקר, קבוצות ריגול איראניות הופכות רשתות שחדרו אליהן לנקודת זינוק לקבוצות אחרות, שמבצעות מתקפות הרס.

בדוגמה אחת, Helix Kitten, המוכרת גם כ־OilRig, אספה מודיעין זמן רב בתוך רשת והעבירה את הגישה ל־Banished Kitten, שפעלה להרס. בדוגמה אחרת, Static Kitten העבירה גישה ל־Storm-1084. במתקפה על ממשלת אלבניה השתתפו ארבע קבוצות. לפי המחקר, ההרס מוסווה לא פעם ככופרה, כלומר נוזקה שמצפינה קבצים ודורשת תשלום, או כמחאה של האקטיביסטים.

"איראן לא מתוחכמת טכנית כמו סין, רוסיה או צפון קוריאה, אבל את מה שחסר לה בתחכום היא משלימה בקצב", אמר החוקר Francis Guibernau. לפי AttackIQ, הקבוצות מגיעות לעיתים ליעדים מוגנים דרך חברות בנות, קבלנים וספקים.

מקור: AttackIQ · (הדוח) AttackIQ

בקצרה

ShadowCloud: Kaspersky חשפה קמפיין ריגול נגד גופי ממשל בדרום־מזרח אסיה, באפריקה ובמרכז אסיה. התוקפים מנצלים את כלי הניהול מרחוק MeshCentral ומסתירים את הפקודות בתעבורה ל־GitHub, ל־SharePoint ול־Ably. לפי החברה, יש סימנים לקשר לקבוצות דוברות סינית. Kaspersky

רומניה: שגרירות רוסיה בבוקרשט מכחישה שהאקרים מטעם רוסיה פרצו למוסד ממשלתי רומני כדי ליירט את המיילים שלו עם נאט"ו והאיחוד האירופי. שירות הביון הרומני ייחס את מתקפת הריגול לקבוצת Turla, שקשורה לשירות הביטחון הפדרלי הרוסי. The Record

AI ואבטחה

גאזט סייבר · 18 בנובמבר 2026

חבילת הסוכנים של מיקרוסופט ב־PyPI הורעלה בגונב סיסמאות

שתי גרסאות מזויפות של agent-framework עלו ביום שלישי בערב ואספו מפתחות ענן. הגרסה הבטוחה האחרונה: 1.26.0.

מישהו העלה ביום שלישי בערב ל־PyPI, מאגר החבילות הרשמי של שפת פייתון, שתי גרסאות זדוניות של agent-framework, ספריית סוכני ה־AI של מיקרוסופט. לפי Wiz, הגרסה 1.26.1 עלתה ראשונה, והגרסה 1.26.2 הגיעה 33 דקות אחריה. שתיהן הוסרו תוך פחות משעה. לחבילה יש כ־41,000 הורדות בשבוע.

הקוד הזדוני מסתתר בקובץ שפייתון מריץ בכל הפעלה, גם כשאף אחד לא קורא לספרייה. הוא אוסף משתני סביבה עם מפתחות וסיסמאות, קובצי הרשאות של Azure, npm, git ו־Docker, ומבקש אסימוני גישה של Azure ושל GitHub Actions. הכול נשלח לשירות הציבורי webhook.site. לפי Wiz, התוקף השתמש בחשבון חינמי, ולכן נקלטו לכל היותר 50 בקשות. גם בהן עלולים להיות מפתחות עובדים.

הדרך שבה הגרסאות עלו עוד לא ידועה. לפי Wiz, אין להן תגית במאגר הקוד של מיקרוסופט, כך שכנראה נבנו מחוץ לתהליך השחרור הרגיל.

> **מה לעשות:** לחפש את הגרסאות 1.26.1 ו־1.26.2 בקובצי הנעילה, ביומני CI ובאימג'ים, לנעול על 1.26.0 ולהחליף כל סוד שהיה זמין במחשב שהתקין אותן.

מקור: Wiz · Socket

מיקרוסופט: אישור אחד בקוד קצר, ותוקף שולט בסוכן הקוד

בניסוי מעבדה, פישינג של קוד מכשיר נתן לחוקרים גישה ל־Copilot CLI, לזיכרון שלו ולמאגרים פרטיים.

בפישינג של קוד מכשיר התוקף לא גונב סיסמה. הוא משכנע את הקורבן להקליד קוד קצר באתר אמיתי, וכך לאשר התחברות שהתוקף עצמו התחיל. חוקרי מיקרוסופט בדקו מה קורה כשהטריק הזה מכוון לסוכן AI, ולא לתיבת מייל.

בניסוי מעבדה על GitHub Copilot CLI, אישור אחד הספיק כדי לשלוט מרחוק בסשן פעיל ולגרום לסוכן להריץ פקודות במחשב של המשתמש, אם השליטה מרחוק הופעלה. החוקרים יכלו גם להוסיף לזיכרון של הסוכן רשומות מטעות, לקרוא סשנים שסונכרנו לענן ולגשת למאגרי קוד פרטיים. לפי מיקרוסופט, זה לא נצפה בשטח, וכל כלי שתומך בשיטת ההתחברות הזו חשוף לאותו טריק.

> **מה לעשות:** להקליד קוד מכשיר רק בהתחברות שהתחלתם בעצמכם, ולבטל ב־GitHub הרשאות OAuth לא מוכרות.

מקור: Microsoft Security

בקצרה

UpdateMITM: חוקרי Lumia הראו שתוקף שמסוגל ליירט תעבורה מוצפנת ברשת ארגונית יכול להחליף עדכון של Cursor, VS Code, Antigravity, Claude Desktop ו־Claude Code בקוד זדוני. לדבריהם, רק Codex ו־ChatGPT, שמתעדכנים דרך החנות של מיקרוסופט, לא נפלו בשיטה הזו. Lumia Security

GitHub ומיקרוסופט שולחות תיקונים, לא עוד התראות AI

בפיילוט על שישה פרויקטים בקוד פתוח, 55 חולשות כבר תוקנו. כל דוח הגיע עם הוכחה והצעת תיקון.

GitHub ומיקרוסופט סרקו שישה פרויקטים בקוד פתוח, ובהם Caddy, Express, ImageMagick ו־Netty, בעזרת מערכת AI של מיקרוסופט בשם Codename MDASH. המערכת סימנה אלפי ממצאים אפשריים. סוכן AI של GitHub סינן אותם, ושבעה חוקרים בדקו כל ממצא שנשאר ביד. למתחזקים הגיעו 99 דוחות פרטיים, כל אחד עם הוכחת היתכנות והצעת תיקון.

עד 15 בנובמבר תוקנו 55 חולשות, ו־14 מהתיקונים כבר נכנסו לגרסאות. המתחזקים של Caddy תיקנו את כל 22 הדוחות שקיבלו בתוך שבוע, ו־ImageMagick תיקנה אחד מהם בתוך 15 דקות. לפי GitHub, המתחזקים מוצפים כיום בדוחות AI שלא נבדקו, והלקח הוא לשלוח רק ממצאים מאומתים, בפרטיות ועם תיקון.

מקור: GitHub Blog · SecurityBrief

בקצרה

Phrack 73: גיליון חדש של מגזין ההאקרים הוותיק, עם 23 מאמרים ראשיים ושמונה קצרים. בין הנושאים: בריחה מקונטיינר Docker, פיתוח ניצול לליבת לינוקס בעידן מודלי השפה, ובריחה מארגז החול של Chromium. Phrack

סייבר ב־X

גאזט סייבר · 18 בנובמבר 2026

על מה מדברים: Java4Shell, Equinor והשיבושים בארה"ב

הסיפורים הבולטים ב־X News בסייבר, 17 עד 18 בנובמבר. חלקם לא אומתו.

החולשה בג'אווה מובילה את הדיון, לצד המתקפה על Equinor והחבילה המורעלת של מיקרוסופט ב־PyPI. לפי סיכום אחר, בכירים אמריקאים אומרים שאין ראיה למתקפת סייבר מאחורי השיבושים האחרונים ב־Apple, בבנקים וברשת הפנימית של NSA. לפי ה־BBC, ה־NSA לא אמרה אם מה שקרה אצלה קשור לחולשה בג'אווה.

מקור: X News · BBC

חולשות מנוצלות ו־KEV

גאזט סייבר · 18 בנובמבר 2026

CISA: תוקפים מנצלים חולשה ב־Puppet Enterprise

החולשה מאפשרת להריץ קוד על השרת שמנהל את כל המחשבים בארגון. פרטי החולשה פורסמו כבר בתחילת החודש.

CISA הוסיפה ביום שלישי לרשימת החולשות המנוצלות את CVE-2026-115731 ב־Puppet Enterprise של Perforce, על סמך ראיות לניצול. Puppet היא מערכת שמנהלת הגדרות ומפיצה שינויים לכל השרתים בארגון, ולכן השרת שלה רב עוצמה.

לפי מאגר החולשות האירופי, הבאג נמצא בקוד שמעבד דוחות שהשרת מקבל מהמחשבים המנוהלים. מי שמחזיק תעודה חתומה של מחשב מנוהל יכול להריץ קוד על השרת. אם השרת מאשר תעודות חדשות אוטומטית, גם תוקף בלי שום הרשאה יכול להשיג תעודה כזו. ציון החומרה: 9.4 מתוך 10. לפי Zero Hunt, קוד הדגמה פורסם כבר ב־3 בנובמבר.

מה לעשות: לעדכן ל־2023.8.13, ל־2025.12.1 או ל־2026.0.1, לכבות אישור אוטומטי של תעודות ולהגביל גישה לפורט 8140.

מקור: CISA · ENISA EUVD · Zero Hunt

כל ידיעה מקושרת למקור. סיכומי X News נכתבים בידי Grok ועלולים לכלול טעויות.