

ניתוח אירוע מתקפת שרשרת אספקה ב-Notepad++ (דצמבר 2025)

תקציר:

מה קרה: תוקפים הצליחו להשתלט על תשתית האירוח (Hosting) של האתר הרשמי, ולא על קוד התוכנה עצמו.

התוקף: הייחוס נעשה לקבוצת ה-APT הסינית Lotus Blossom (מוכרת גם בשמות Billbug או Violet Typhoon). הקבוצה ידועה בפעולות ריגול ממוקדות.

וקטור התקיפה: השתלטות על תשתית האירוח של האתר הרשמי ← יירוט בקשות לעדכון תוכנה, וניתובן לשרתים בשליטת הגורם הזדוני ← הגשת קבצי עדכון נגועים במקום קבצים לגיטימיים ← יצירת Backdoor חדש בשם Chrysalis, המאפשר RCE ואיסוף מידע.

ציר זמן:

לוח זמנים: הפעילות העוינת התרחשה בין יוני 25 לדצמבר 25.
סטטוס נוכחי: בינואר 26 שוחררו עדכונים שמטרתם לחסום את הפרצה (v8.9.1 ו-v8.9.2).

השפעה עסקית (Business Impact):

- פגיעה בשלושת ערכי ה-CIA:
 - Integrity (שלמות):** פגיעה עקב החלפת קבצי מקור רשמיים בקוד זדוני.
 - Confidentiality (סודיות):** סיכון דלף מידע רגיש, סיסמאות וגישת מרחוק לארגונים שהתקינו את העדכון.
 - Availability (זמינות):** השבתת מנגנון העדכונים וצורך בחסימת התוכנה בארגונים עד לניקוי התשתית.
- פגיעה במוניטין ובאמון:** שחיקת האמות במוצר Notepad++ ככלי עבודה בטוח, ופגיעה רחבה יותר בתפיסת הביטחון של כלי קוד פתוח בארגונים.

- **עלויות תפעוליות:** משאבים כבדים שהופנו ל-IR, ניקוי תחנות קצה בארגונים נפגעים, ומעבר תשתיות של צוות הפיתוח.
 - **סיכוני ציות (Compliance):** חשיפה לאי-עמידה בתקני אבטחה (כמו ISO 27001) עבור ארגונים שלא זיהו וטיפלו בגרסאות הנגועות בזמן.
-

היבטי ממשל וניהול סיכונים GRC:

- כשל בבקרת אימות:** הגרסאות הישנות של מנגנון העדכון (WinGUp) לא ביצעו אימות מספק של חתימות דיגיטליות לפני ההתקנה, מה שאפשר להריץ את הקבצים המתחזים.
- סיכוני תשתית אירוח:** הפריצה התאפשרה דרך ספק האירוח, מה שממחיש את החשיבות של בחינת רמת האבטחה של ספקי תשתית (SaaS/IaaS) כחלק מניהול סיכונים ארגוני.
- תגובה לאירוע:** עם גילוי האירוע, המפתחים ביצעו מספר צעדים מתקנים:
- מעבר לספק אירוח חדש עם רמת אבטחה גבוהה יותר.
 - החלפת (Rotation) כל פרטי הגישה והסיסמאות.
 - הקשחת מנגנון העדכון בגרסאות החדשות (v8.9.2), כך שיחייב בדיקת חתימות ותעודות אבטחה באופן מחמיר.
-

המלצות:

למשתמשים ולמנהלי מערכות מומלץ לוודא שהם משתמשים בגרסה העדכנית ביותר של התוכנה (לפחות v8.9.1 ומעלה) **שהורדה ישירות מהאתר החדש**, ולא להסתמך על תהליכי עדכון אוטומטיים מגרסאות ישנות שייתכן ועדיין מופנים לתשתית הנגועה.