

כיתוח אירוע מתקפת שרשרת אספקה ב-++pad (דצמבר 2025)

תקציר:

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

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

וクトור התקיפה: השתלטות על תשתית האירוח של האתר הרשמי ← "ירוט בקשנות לעדכון תוכנה, וניתובן לשרתים בשליטת הגורם הזרים" ←agation קבצי עדכון נגעים במקום קבצים לגיטימיים ← יצירת Backdoor חדש בשם Chrysalis, המאפשר RCE ואיסוף מידע.

ציר זמן:

לוח זמנים: הפעולות העוינית התרחשו בין יוני 25 לדצמבר 25.

סטטוס נכון: בינואר 26 שוחררו עדכונים שמטרתם לחסום את הפרצה (v8.9.1 ו-v8.9.2).

השפעה עסקית (Business Impact):

- **פגיעה בשלושת ערכי ה-CIA:**
- **פגיעה[Integrity] (שלמות):** פגיעה עקב החלפת קבצי מקור רשמיים בקוד זמני.
- **פגיעה[Confidentiality] (סודיות):** סיכון דלף מידע רגייש, סיסמאות וגישה מרחוק לארגונים שהתקינו את העדכון.
- **פגיעה[Availability] (זמןנות):** השבתת מנגןן העדכנים וצרוך בחסימת התוכנה בארגונים עד לניקוי התשתיות.
- **פגיעה במוניטין ובאמון:** שחיקת האמות ב מוצר ++pad Notepad כלי עבודה בטוח, ופגיעה רחבה יותר בתפיסת הביטחון של כל קוד פתוח בארגונים.

- **עלויות תפעוליות:** משאבים כבדים שהופנו ל-RIO, ניקוי תחנות קצה בארגונים נגעים, ומעבר תשתיות של צוות הפיתוח.
 - **סיכון ציות (Compliance):** חשיפה לא-עמידה בתקני אבטחה (כמו ISO 27001) עבור ארגונים שלא זיהו וטיפלו בגרסאות הנגעות בזמן.
-

היבטי משל וניהול סיכוניים GRC:

כשל בבדיקה אימומת: הגרסאות הישנות של מנגנון העדכון (WinGUp) לא ביצעו אימומת מספק של חתימות דיגיטליות לפני התקינה, מה שאפשר להריץ את הקבצים המתחזים.

סיכון תשתית אירוח: הפריצה התאפשרה דרך ספק האירוח, מה שמחיש את החשיבות של בדיקת רמת האבטחה של ספק תשתיות (SaaS/IaaS) כחלק מניהול סיכוניים ארגוני.

תגובה לאירוח: עם גילוי האירוח, המפתחים ביצעו מספר צעדים מתוקנים:

- מעבר לשירות חדש עם רמת אבטחה גבוהה יותר.
 - החלפת (Rotation) כל פרטי הגישה והסיסמאות.
 - הקשה מנגן העדכון בגרסאות חדשות (8.9.2), כך שיחיב בדיקת חתימות ותעודות אבטחה באופן מחמיר.
-

המלצות:

למשתמשים ולמנהל מערכות מומלץ לוודא שהם משתמשים בגרסה העדכנית ביותר של התוכנה (לפחות 8.9.1 ומעלה) **שהורדה ישירות מהאתר החדש**, ולא להסתמך על תהליכי עדכון אוטומטיים מגרסאות ישנות שייתכן ועדין מופנים לתשתית הנגעה.