30/06/2024
כ"ד סיון תשפ"ד
סימוכין: 1755

פעילות קבוצת הכופרה TellYouThePass

תקציר

1. ממידע בידי מערך הסייבר הלאומי עולה כי הגורמים העומדים מאחורי הכופרה המוכרת בשם TellYouThePass מנצלים בצורה משמעותית את פגיעות CVE-2024-4577 בשרתי PHP על גבי מערכת הפעלה Windows.
2. להתרעה זו מצורף קובץ מזהים, העשוי לאפשר זיהוי של פעילות הקבוצה. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.

פרטים

1. ימים בודדים לאחר פרסום הפגיעות, תוקפים החלו לסרוק שרתים הפגיעים לחולשה זו על מנת לבצע מתקפות כופרה.
2. פעילות התקיפה מרוכזת כרגע במזרח אסיה, מאחר והדיווח המקורי עסק בתשתית הפועלת בשפות מאזור זה, אולם ייתכן והפגיעות ניתנת למימוש גם בשרתים הפועלים עם שפות שונות מאלו שצוינו בפרסום המקורי.
3. הקבוצה המפעילה את כופרת TellYouThePass אינה זרה למימוש פגיעויות בשרתי Web. באוקטובר 2023 נוהל קמפיין תקיפה ע"י אותה קבוצה תוך ניצול של פגיעות CVE-2023-46604 (חולשה בתוכנת Apache ActiveMQ), ובעבר ביצעה הקבוצה שימוש בחולשה CVE-2021-44228 (חולשה בתוכנת Apache Log4j).
4. הכופרה עושה שימוש בחולשות RCE (Remote Code Execution) בשרתי אינטרנט כדי להשיג גישה ולבצע הצפנה. בקמפיין הנוכחי, בעזרת החולשה מורד קובץ HTA משרת בשליטת התוקף, הכולל VBScript שמכיל את קובץ ההרצה של הכופרה, מקודד בפורמט base64.

דרכי התמודדות

1. ראו התרעת מערך הסייבר הלאומי לגבי הפגיעות ב-PHP בקישור מס' 1. מומלץ מאד לבחון ולעדכן את התוכנה לגרסה עדכנית בהקדם האפשרי.

2. להתרעה זו מצורף קובץ מזהים. מומלץ מאד לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.

מקורות

1. https://www.gov.il/he/pages/alert_1744

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה בלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.