29/07/2024
כ"ג תמוז תשפ"ד
סימוכין: 1780

פגיעות בתוכנת WhatsApp for Windows

תקציר

1. לאחרונה פורסם כי הגרסה העדכנית של תוכנת WhatsApp for Windows מאפשרת הפעלה של מספר סוגי קבצים ללא התרעה.
2. תוקפים עלולים לנצל פגיעות זו להרצת קוד על עמדת המשתמש הנמען.

פרטים

1. לפי הפרסומים, התוכנה מאפשרת הפעלת קבצי PHP ו-Python בעלי סיומות .php, .pyz, .pyzw. ללא התרעה.
2. ניצול פגיעות זו לרעה מחייב שהעמדה תכיל התקנה של Python או PHP.

דרכי התמודדות

1. אם אמצעי אבטחה בעמדה מאפשר למנוע הפעלת/פתיחת קבצים לפי סיומת, מומלץ לבחון שימוש בו על מנת למנוע הפעלת הקבצים.
2. אם לארגון יש אמצעי אבטחה להורדת קבצים מהרשת, ניתן לבחון חסימת קבצים עם סיומות אלו.
3. מומלץ להתריע בפני כל המשתמשים הרלוונטיים על הסיכון הפוטנציאלי בפתיחת קבצים מסוג זה.
4. מומלץ לבחון האם הארגון יכול להשתמש בגרסת ה-Web של התוכנה באמצעות דפדפן, במקום בתוכנה המותקנת על העמדה.
5. לפי הפרסום, נכון למועד פרסום התרעה זו החברה לא מתכוונת לתקן פגיעות זו.

מקורות

1. https://www.bleepingcomputer.com/news/security/whatsapp-for-windows-lets-python-php-scripts-execute-with-no-warning/

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.