



22 בדצמבר 2022  
כ"ח בכסלו תשפ"ג  
סימוכין: ב-ס-1520

## פגיעויות בשרתי Exchange מנוצלות לתקיפות בעולם

### תקציר



1. פגיעויות בשרתי Exchange שפרסמה חברת מיקרוסופט בחודש נובמבר 2022 מנוצלות בפועל לתקיפות בעולם.
2. מומלץ לבחון ולהתקין בהקדם האפשרי את עדכוני האבטחה הרלוונטיים.

### פרטים



1. בתחילת חודש אוקטובר 2022 פורסם מידע לגבי 2 פגיעויות Zero Day המשמשות לתקיפת שרתי Exchange.
2. הפגיעויות זוהו כ-CVE-2022-41040 ו-CVE-2022-41082 וצירוף של שתיהן (שזכה לכינוי ProxyNotShell), איפשר לתוקף מרוחק ומזוהה הרצת קוד על השרת.
3. השלב הראשון כלל תקיפה מסוג SSRF, והשני גישה מרוחקת ל-PowerShell על השרת.
4. בתחילה החברה הוציאה מעקפים שונים לפגיעויות, ובחודש נובמבר 2022 פרסמה מקבץ של 6 עדכוני אבטחה לשרתי Exchange, הכולל את 2 הפגיעויות הללו.
5. לאחרונה פורסם כי דווחו בעולם מקרים בהם תוקפים עשו שימוש בפגיעות אחרת מתוך עדכון נובמבר, המזוהה כ-CVE-2022-41080, למימוש השלב הראשון בתקיפה.
6. פגיעות זו מאפשרת העלאת הרשאות לתוקף מרוחק ומזוהה.
7. המשמעות היא כי שיטות המעקף שהומלצו בעבר על ידי החברה כנגד CVE-2022-41040, אינן יעילות עוד למניעת תקיפת השרת בשיטה החדשה.
8. התקיפות בשיטה החדשה שימשו כוקטור תקיפה ראשוני באירועי כופרה.

ניתן לשותף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

## דרכי התמודדות



1. מומלץ מאד לבחון ולהתקין על השרתים את עדכוני האבטחה שפורסמו בחודש נובמבר 2022. ראו קישור מס' 1 בסעיף "מקורות" להלן.
2. מומלץ לבחון ולהטמיע המלצת החברה להגביל גישה מרחוק ל-PowerShell בשרת ה-Exchange למנהלני השרת בלבד, כפי שמוסבר בקישור מס' 2 בסעיף "מקורות" להלן.

## מקורות



1. <https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d>
2. <https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps&viewFallbackFrom=exchange-ps%22%20%5C%20%22use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user>
3. <https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/>

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, 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.



ניתן לשותף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים