

27 אפריל 2020  
ג' אייר תש"פ  
סימוכין:ב-ס-1071

## פגיעות Zero-Day ב-Sophos XG Firewall

### תקציר



לאחרונה דווחה חברת Sophos על פגיעות Zero Day ב-XG Firewall מתוצרתה. בתנאים מסוימים הפגיעות ניתנת לניצול מרחוק על מנת להריץ קוד על הציוד, וללא צורך בהזדהות. מומלץ לבחון העדכון ולהתקינו בהקדם האפשרי.

### פרטים



- מקור הפגיעות בתקיפה מסוג SQL Injection, הניתנת למימוש ללא הזדהות.
- התקיפה ניתנת למימוש אם ה-Firewall מוגדר באחד מן האופנים הבאים:
  - ממשק הניהול (HTTPS Admin Service) חשוף לרשת (WAN Zone).
  - פורטל המשתמשים חשוף לרשת.
  - ה-Firewall מוגדר ידנית כך שאחד משירותיו (לדוגמה, SSLVPN), חשוף לרשת באותו ממשק כמו אחד הממשקים בסעיפים הקודמים.
- הפגיעות שימשה למתקפה כנגד הציוד, שמטרתה דלף מידע לתוקף. מידע זה כולל שמות משתמש וסיסמאות המוגדרים מקומית בציוד, כגון מנהלנים מקומיים, משתמשי פורטל מקומיים, וחשבונות המשמשים לגישה מרחוק. סיסמאות המוגדרות במערכות הזדהות חיצוניות כגון AD או LDAP לא דלפו.

## 4. כל הגרסאות של ה-Firewall פגיעות.

**דרכי התמודדות**

1. החברה דחפה עדכון אוטומטי לכל ציוד שהוגדר לכך. מומלץ לוודא כי העדכון הותקן, ואם לאו, לוודא התקנה בהקדם האפשרי לאחר בחינה.
  2. לאחר התקנת העדכון, תופיע בממשק הניהול הודעה האם הציוד הותקף טרם העדכון. אם ההודעה חיובית, מומלץ:
    1. לאתחל סיסמאות מנהלנים.
    2. לאתחל את הציוד.
    3. לאתחל את כל סיסמאות המשתמשים המקומיים.
    4. אם נעשה שימוש בסיסמאות אלו בציוד אחר, מומלץ לשנותן, למרות שהסיסמאות נשמרות כ-Hash בציוד.
  3. להתרעה זו מצורף קובץ מזהים עבור הקמפיין שבו נעשה שימוש בפגיעות לתקיפת ציוד מסוג זה. מומלץ לנטרם במערכות הארגוניות.
- לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

**מקורות**

1. <https://community.sophos.com/kb/en-us/135412>
2. <https://news.sophos.com/en-us/2020/04/26/asnarok/>

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.



בברכה,

